



# **SPECTRUM<sup>®</sup>**

**Portable Management Application**

**for the**

**FRX4000, FRX6000, and SmartSwitch 1800**

**User's Guide**

**CABLETRON**  
*SYSTEMS*

The Complete Networking Solution™



## Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

## Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © 1998 by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9032412-E2 April 1998

Cabletron Systems, Inc.  
P.O. Box 5005  
Rochester, NH 03866-5005

**SPECTRUM**, **MiniMMAC**, **FNB**, **Multi Media Access Center**, and **DNI** are registered trademarks, and **Portable Management Application**, **IRM**, **IRM2**, **IRM3**, **IRBM**, **ESXMIM**, **ETSMIM**, **EMME**, **EMM-E6**, **ETWMIM**, **FDMMIM**, **FDCMIM**, **MicroMMAC**, **MRXI**, **MRXI-24**, **NB20E**, **NB25E**, **NB30**, **NB35E**, **NBR**, **SEHI**, **STHI**, **TRBMIM**, **TRMM**, **TRMM-2**, **TRMM-4**, **TRMMIM**, **TRXI**, **Media Interface Module**, **MIM**, and **Flexible Network Bus** are trademarks of Cabletron Systems, Inc.

**UNIX** and **OPENLOOK** are trademarks of Unix System Laboratories, Inc. **OSF/Motif** and **Motif** are trademarks of the Open Software Foundation, Inc. **X Window System** is a trademark of X Consortium, Inc. **Ethernet** and **XNS** are trademarks of Xerox Corporation. **Apple** and **AppleTalk** are registered trademarks of Apple Computer, Inc. **Banyan** is a registered trademark of Banyan Systems, Inc. **DECnet** is a registered trademark of Digital Equipment Corporation. **Novell** is a registered trademark of Novell, Inc. **CompuServe** is a registered trademark of CompuServe. **Sun Microsystems** is a registered trademark, and **Sun**, **SunNet**, and **OpenWindows** are trademarks of Sun Microsystems, Inc.

# Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867-0505.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.
  - (b) This computer software may be:
    - (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;
    - (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;
    - (3) Reproduced for safekeeping (archives) or backup purposes;
    - (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;
    - (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and
    - (6) Used or copied for use in or transferred to a replacement computer.
  - (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.
  - (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.
  - (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.

## Chapter 1 Introduction to SPMA for the FRX4000, FRX6000, and SmartSwitch 1800

Using this Guide.....	1-2
What's NOT in the FRX User's Guide . . .	1-4
Conventions.....	1-4
Screen Displays .....	1-5
Using the Mouse .....	1-6
Getting Help .....	1-7
FRX4000, FRX6000, and SmartSwitch 1800 Firmware.....	1-8
Year 2000 Compliance .....	1-8

## Chapter 2 Using the FRX4000, FRX6000, and SmartSwitch 1800 Hub View

Using the Hub View .....	2-1
Navigating Through the Hub View .....	2-2
Port and Module Color Codes.....	2-4
Using the Mouse in a Hub View Module.....	2-6
The Hub View Front Panel .....	2-7
Monitoring Hub Performance.....	2-10
Selecting a Port Display Form.....	2-12
Viewing Device Information.....	2-16
Configuring RLP Protocols.....	2-16
Configuring Serial Port Protocols.....	2-19
Viewing Serial Port Information.....	2-20
Serial Port Pin Status.....	2-21
Viewing LAN Port Information.....	2-23
Viewing Statistics .....	2-24
RLP Health.....	2-24
Serial Port Health.....	2-26
LAN Card Health .....	2-27
Viewing Statistics Thresholds .....	2-29
RLP Statistics Thresholds .....	2-29
Serial Port Statistics Thresholds .....	2-30
Managing the Hub.....	2-32
Setting the Polling Intervals .....	2-32
Enabling and Disabling Serial Ports.....	2-34
Applying Port-level Changes.....	2-34

## Chapter 3 Configuring the Trap Table

About Traps.....	3-1
Launching the Trap Table.....	3-1
Configuring Traps .....	3-3
Trap Messages.....	3-4

## Chapter 4 Configuring the Subscriber Table

About Subscriber IDs.....	4-1
Accessing the Subscriber Table .....	4-2
Configuring the Subscriber Table .....	4-3
Configuring Routing Table Entries.....	4-5
Configuring Address Table Entries .....	4-6
Adding or Modifying Subscriber Table Entries .....	4-6
Deleting Table Entries.....	4-8

## Chapter 5 Frame Relay Status and Configuration

Configuring Frame Relay Ports.....	5-2
Port Configuration .....	5-2
Changing Configuration Values .....	5-8
Applying Port-level Changes.....	5-8
DLCI Rate Configuration.....	5-8
Changing DLCI Rate Values.....	5-11
Applying Port-level Changes.....	5-12
Frame Relay Backup Groups .....	5-12
Configuring Frame Relay Backup Groups .....	5-13
Changing Backup Group Values .....	5-14
Configuring Logical Ports.....	5-15
Changing Configuration Values .....	5-20
Applying Port-level Changes.....	5-20
Viewing Frame Relay Status.....	5-20
Management Stats.....	5-21
Congestion Stats .....	5-22
Errors.....	5-23

## Chapter 6 X.25 Status and Configuration

Configuring X.25 Physical Ports .....	6-2
Changing Configuration Values .....	6-8
Applying Port-level Changes.....	6-8
Viewing X.25 Status .....	6-8
Management Stats.....	6-8
Congestion Stats .....	6-9
Errors.....	6-10

**Chapter 7 SNA Status and Configuration**

Configuring SNA Ports ..... 7-2

    SDLC Port Configuration ..... 7-2

        Changing Configuration Values ..... 7-7

        Applying Port-level Changes..... 7-7

    SDLC PU Configuration ..... 7-7

        Changing SDLC PU Subscriber Values ..... 7-10

        Applying Port-level Changes..... 7-10

    SDLC PU LLC2 Configuration..... 7-10

        Changing SDLC PU LLC2 Values ..... 7-14

        Applying Port-level Changes..... 7-15

    SDLC Link Station Configuration ..... 7-15

        Changing SDLC Link Station Values ..... 7-18

        Applying Port-level Changes..... 7-18

Configuring LLC2 ..... 7-18

    Changing Configuration Values ..... 7-23

    Configuring LLC2 Host Connections ..... 7-24

        Changing Host Connections ..... 7-26

Viewing SDLC Status ..... 7-26

    SDLC Port Statistics ..... 7-26

    SDLC Link Station General Statistics ..... 7-29

    SDLC Link Station Rx and Tx Statistics..... 7-30

**Chapter 8 BSC Interactive Configuration**

Configuring BSCI Ports ..... 8-1

    Changing BSCI Port Configuration Values ..... 8-6

    Applying Port-level Changes..... 8-6

BSCI Subscriber ID Information ..... 8-7

    Adding or Modifying BSCI Subscriber Information ..... 8-9

    Applying Port-level Changes..... 8-9

Configuring BSCI Devices ..... 8-9

    Adding or Modifying BSCI Device Information ..... 8-11

    Applying Port-level Changes..... 8-11

**Chapter 9 IP Interface Configuration**

Configuring IP Node Defaults ..... 9-1

Configuring IP Interfaces ..... 9-2

    Configuring IP Interface Secondary Addresses ..... 9-9

Adding or Modifying IP Interfaces ..... 9-11

    Adding or Modifying Secondary Addresses ..... 9-12

## **Chapter 10 IPX Interface Configuration**

Configuring IPX Node Defaults.....	10-1
Configuring IPX Interfaces .....	10-2
Adding or Modifying IPX Interfaces.....	10-9
Configuring IPX Static Routes.....	10-10
IPX Static SAP Configuration.....	10-10
Adding or Modifying Static SAP Routes.....	10-11
IPX Static Route Configuration .....	10-12
Adding or Modifying IPX Static Routes.....	10-14

## **Chapter 11 Bridge Configuration**

Configuring Device-Level Bridging Parameters .....	11-1
Changing Configuration Values .....	11-3
Configuring Bridge Ports .....	11-4
Configuring Frame Relay Bridge Ports.....	11-4
Adding or Modifying Frame Relay Bridge Ports.....	11-7
Configuring LAN Bridge Ports .....	11-7
Adding or Modifying LAN Bridge Ports .....	11-9

## **Chapter 12 SmartSwitch 1800 Voice Configuration**

Configuring System-Level Voice Parameters.....	12-2
Changing Parameter Values .....	12-5
Speed Dial Configuration.....	12-5
Adding or Modifying Speed Dial Numbers .....	12-7
Configuring Voice Ports .....	12-8
Changing Port Configuration Values .....	12-15
Applying Port-level Changes .....	12-15
Configuring Voice Interfaces .....	12-15
Adding or Modifying Voice Interfaces.....	12-17
Viewing Voice Statistics.....	12-18

## **Appendix A FRX4000, FRX6000, and SmartSwitch 1800 MIB Components**

IETF MIB Support .....	A-1
CSI Netlink MIB Support .....	A-2

## **Index**



# Introduction to SPMA for the FRX4000, FRX6000, and SmartSwitch 1800

*Using this Guide; manual conventions; contacting the Cabletron Systems' Global Call Center; firmware versions supported by SPMA*

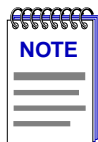
---

Your SPMA for the FRX4000, FRX6000, and the SmartSwitch 1800 management module provides management support for the FRX4000 stand-alone frame relay access device; its larger cousin, the FRX6000 scalable chassis; and the innovative SmartSwitch 1800 frame relay access device. These devices are high-performance Frame Relay products that combine the capabilities of a frame relay access device (FRAD) and a router in one box.

The **FRX4000** is designed for smaller branch offices that require high performance to integrate with larger networks over frame relay at access rates up to T1 and beyond. It supports up to eight serial interfaces (RS232, V.35, or RS422) and one LAN (Ethernet or Token Ring) interface, and is available in a variety of models depending on the combination of LAN interface and serial protocols you need.

The **FRX6000** is ideal for data centers and concentration sites because of its scalable rackmount chassis. Its eight slots can support up to two LAN interface cards and 48 serial interfaces, or as many as 56 (with a single LAN interface) or 64 (with no LAN interface) serial interfaces. Up to eight ports can operate at T1 speeds, and as many as six can operate at E1 speeds. Expansion cards are available for Ethernet or Token Ring LAN support, and for RS232, V.35, or RS422 serial interfaces; a wide variety of protocol support is also provided.

The **SmartSwitch 1800** is a high performance, multiprotocol frame relay access device that provides multimedia support by adding voice technology to traditional data applications. Designed for branch offices, it supports four serial interfaces for WAN and local connectivity (RS232, V.35, or RS422), two analog RJ45 voice channels, and one LAN (Ethernet or Token Ring) interface.



*The protocol support functions which are available via your SPMA application will vary depending on the protocol support you have purchased for your FRX or SmartSwitch 1800 device and the version of firmware you are running. For more information about available protocols and the current availability of SPMA support for those protocols, contact Cabletron Systems' Global Call Center.*

Note that because the FRX4000 and FRX6000 provide virtually the same functionality, they will be referred to collectively throughout this manual as the FRX. Where significant differences exist, they will be noted.



*SPMA support for the FRX4000, FRX6000 and SmartSwitch 1800 can also be used to manage new Frame Relay Modules for the SmartSwitch 9000 that are based on FRX technology: the 9W410 (Ethernet) and the 9W450 (Token Ring). Please note, however, that at the time of this SPMA release these Frame Relay modules were not yet available; therefore, this software has not been tested against them, and supplied functionality will be limited. Full SmartSwitch 9000 Frame Relay Module support will be included in a future release of SPMA.*

## Using this Guide

Your SPECTRUM Portable Management Application (SPMA) for the FRX4000, FRX6000, and SmartSwitch 1800 consists of a number of different applications, each of which provides a portion of the overall management functionality. Each of these applications can be accessed from the icon menu (if you are using a management platform) and from the Stand-alone Launcher or the command line (if you are running in stand-alone mode); in addition, several applications can also be accessed from within the Hub View, a graphical display of the device and its installed interfaces.

This *User's Guide* describes how to use most of the applications included with the module; note that the instructions provided in this guide apply to the FRX or SmartSwitch module regardless of the operating system or management platform you are using. Instructions for launching each individual function from the command line (stand-alone mode) are also included in each chapter.

Following is a description of the applications covered in this guide; while we provide as much background information as we can, we do assume that you're familiar with Ethernet, Token Ring, Frame Relay, and X.25 networks, and with general network management concepts:

- Chapter 1, **Introduction**, provides a list of related documentation, describes certain software conventions, and shows you how to contact the Cabletron Systems Global Call Center.
- Chapter 2, **Using the Hub View**, describes the visual display of each device and explains how to use the mouse within the Hub View; some basic functions (changing the Hub View display, opening menus and windows, enabling and

disabling serial ports, and so on) available only from within the Hub View are also described. You can access the Hub View application from the icon menu or the command line.

- Chapter 3, **Trap Table**, describes how to configure the device's trap table, which controls which management stations will receive traps from a selected device. The Trap Table application is accessible from the Hub View.



*Since these devices' trap tables contain some additional functionality not found in other Cabletron devices, its operation is described here. Note that the **Trap Table** chapter included in the **SPMA Tools Guide** does not apply to these devices.*

- Chapter 4, **Configuring the Subscriber Table**, describes how to add, modify, and delete entries in the subscriber table, which controls the operation of virtual circuits across the frame relay network. You can access the Subscriber Table application from the Hub View.
- Chapter 5, **Frame Relay Status and Configuration**, describes how to configure serial ports set to operate using the frame relay protocol (including DLCI configuration); it also describes how to configure logical ports and frame relay backup groups. Frame relay-specific management, congestion, and error statistics are also described. Frame relay status and configuration options are available from the Hub View.
- Chapter 6, **X.25 Status and Configuration**, describes how to configure serial ports for X.25 protocol support and provides detailed information about management, congestion, and error statistics available on the ports. X.25 status and configuration options are available from the Hub View.
- Chapter 7, **SNA Status and Configuration**, describes how to configure SNA ports and provides physical unit and link station parameters. SDLC-specific port and general statistics are also provided. SNA status and configuration options are available from the Hub View.
- Chapter 8, **BSC Interactive Configuration**, describes how to configure binary synchronous communications (BSC) Interactive ports and provides BSCI Subscriber and Device information. BSCI configuration options are available from the Hub View.
- Chapter 9, **IP Interface Configuration**, describes how to configure an IP Interface to allow the Internet Protocol (IP) to be executed over a frame relay, X.25, or LAN interface. IP Interface options are available from the Hub View.
- Chapter 10, **IPX Interface Configuration**, describes how to configure an IPX Interface to allow connections to Novell IPX networks. IPX Interface options are available from the Hub View.
- Chapter 11, **Bridge Configuration**, describes how to set up a bridge interface and provides detailed information on configuring device-level bridging parameters. It also describes how to configure frame relay and LAN bridge ports. Bridging configuration options are available from the Hub View.

- Chapter 12, **SmartSwitch 1800 Voice Configuration**, describes how to configure the two voice ports on the SmartSwitch 1800 and provides statistical information about voice traffic being transmitted across those ports.
- Appendix A, **FRX4000, FRX6000, and SmartSwitch 1800 MIB Components**, lists the IETF and proprietary MIBs supported by these devices.

## What's NOT in the FRX User's Guide . . .

The following standard SPMA tools are available through the FRX4000, FRX6000 and SmartSwitch 1800 modules and are explained in the *SPECTRUM Portable Management Application Tools Guide*:

- Charts and Meters
- MIB I, II
- MIBTree
- Utilities (Global Community Names, Find MAC Address, and TFTP)

Charts, Graphs, and Meters are accessible from the Hub View and the command line; the Utilities and MIBTree applications are accessible from the platform console window Tools menu or the Stand-alone Launcher applications menu, and MIBTree can also be launched from the command line; and MIB I, II is available from the icon menu, the Hub View, or the command line.

Instructions on discovering Cabletron devices, creating icons, and accessing the icon menus within your management platform are included in your *Installing and Using SPECTRUM for...* guide. If you are using SPMA for the FRX or SmartSwitch 1800 in stand-alone mode — that is, without benefit of a specific network management system — instructions for starting each application from the command line are included in each chapter of this guide and the *SPMA Tools Guide*.

## Conventions

SPECTRUM Portable Management Applications — including the FRX and SmartSwitch 1800 module — can work with a number of different network management systems running on several different operating systems and graphical user interfaces. This versatility presents two documentation problems: first, there is no standard terminology; and second, the appearance of the windows will differ based on the graphical interface in use. For the sake of consistency, the following conventions will be followed throughout this and other SPMA guides.

## Screen Displays

SPMA runs under a variety of different operating systems and graphical user interfaces. To maintain a consistent presentation, screen displays in this and other SPMA guides show an OSF/Motif environment. If you're used to a different GUI, don't worry; the differences are minor. Buttons, boxes, borders, and menus displayed on your screen may look a bit different from what you see in the guide, but they're organized and labelled the same, located in the same places, and perform the same functions in all screen environments.

Some windows within SPMA applications can be resized; those windows will display the standard window resizing handles employed by your windowing system. Resizing a window doesn't resize the information in the window; it just changes the amount of information that can be displayed (see [Figure 1-1](#)). When you shrink a window, scroll bars will appear as necessary so that you can scroll to view all the information that is available.

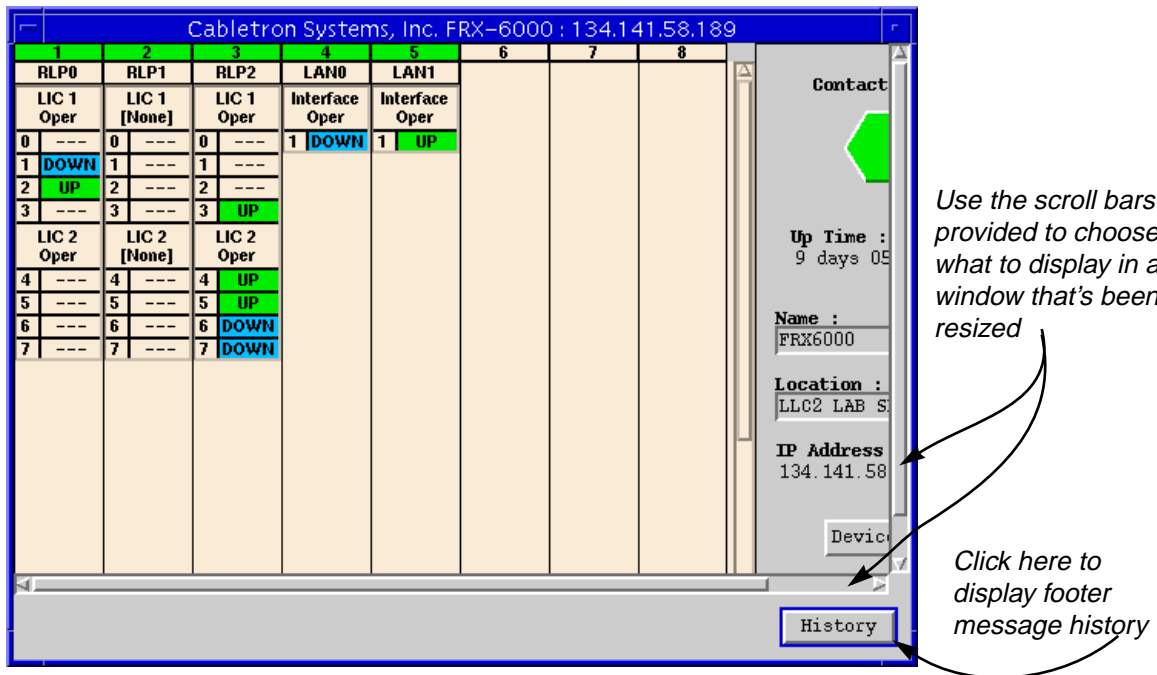
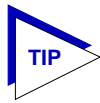


Figure 1-1. Window Conventions

Some windows will also contain a `History` button; selecting this button launches a History window ([Figure 1-2](#)) which lists all footer messages that have been displayed since the window was first invoked. This window can help you keep track of management actions you have taken since launching a management application.



The FRX Hub View application currently prints few footer messages (most of which relate to loss of contact with the device), so little information will typically be recorded in the History window; future releases will expand this feature.



Figure 1-2. The History Window

## Using the Mouse

The UNIX mouse has three buttons. Procedures within the SPMA document set refer to these buttons as follows:

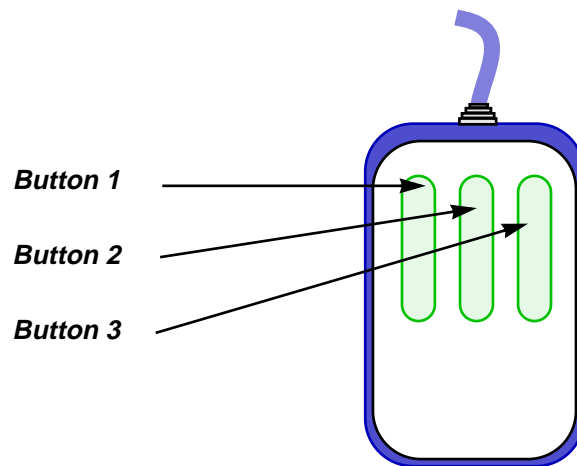


Figure 1-3. Mouse Buttons

If you're using a two-button mouse, don't worry. SPMA doesn't make use of mouse button 2. Just click the left button for button 1 and the right mouse button when instructed to use mouse button 3.

Whenever possible, we will instruct you on which mouse button to employ; however, menu buttons within SPMA applications will operate according to the convention employed by the active windowing system. By convention, menu buttons under the Motif windowing environment are activated by clicking the left mouse button (referred to as mouse button 1 in SPMA documentation), and there is no response to clicking the right button (mouse button 3). Under OpenWindows, menu buttons can be activated by clicking the right button, and convention dictates that the left button activates a default menu option; within SPMA, that default option will also display the entire menu. Because of this difference, references to activating a menu button will not include instructions about which mouse button to use. All other panels from which menus can be accessed, and all buttons which do not provide access to menus, will operate according to SPMA convention, as documented.

## Getting Help

If you need technical support related to SPMA, or if you have any questions, comments, or suggestions related to this manual or any of our products, please feel free to contact the Cabletron Systems Global Call Center. Before calling, please have the following information ready:

- The product name and part number.
- The version number of the program that you need help with. SPMA is modular, which means each application will have a specific revision number. Where applicable, an INFO button provides the version number; you can also view the version number for any application by typing the command to start the application followed by a `-v`.

You can contact Cabletron Systems Global Call Center via any of the following methods:

By phone: Monday through Friday between 8 AM and 8 PM  
Eastern Standard Time at (603) 332-9400.

By mail: Cabletron Systems, Inc.  
PO Box 5005  
Rochester, NH 03866-5005

By Internet mail: support@ctron.com

FTP: ftp.ctron.com (134.141.197.25)

*Login* anonymous  
*Password* your email address

By BBS: (603) 335-3358

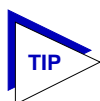
Modem Setting      8N1: 8 data bits, 1 stop bit, No parity

For additional information about Cabletron Systems products, visit our World Wide Web site: <http://www.cabletron.com/>. For technical support, select **Service and Support**.

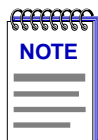
## FRX4000, FRX6000, and SmartSwitch 1800 Firmware

SPMA for the FRX4000, FRX6000, and the SmartSwitch 1800 has been beta-tested against released firmware version 4.0 only; if you have a different version of firmware and experience problems running SPMA, contact Cabletron Systems' Global Call Center for upgrade information.

This SPMA operates with FRX and SmartSwitch 1800 firmware versions 3.3 or greater. However, due to SNMP limitations in firmware versions prior to 4.0, it is recommended that this SPMA be used in conjunction with firmware 4.0 or greater.



*As a general rule, firmware versions (and software support) for new products are liable to change rapidly; contact Cabletron Systems' Global Call Center for information about the latest customer release of firmware and software available.*



*SPMA support for the FRX4000, FRX6000 and SmartSwitch 1800 can also be used to manage new Frame Relay Modules for the SmartSwitch 9000 that are based on FRX technology: the 9W410 (Ethernet) and the 9W450 (Token Ring). Please note, however, that at the time of this SPMA release these Frame Relay modules were not yet available; therefore, this software has not been tested against them, and supplied functionality will be limited. Full SmartSwitch 9000 Frame Relay Module support will be included in a future release of SPMA.*

## Year 2000 Compliance

Previous users of SPMA will note a few display changes related to Year 2000 compliance. All SPMA applications now have the ability to display a four-digit year value where this information is available. For example, the Stand-alone Launcher window — which uses your workstation's system time value to display the time and date of the last contact change — will now display these date values with eight digits (05/31/1998) instead of six (05/31/98).

Please keep in mind, however, that SPMA's ability to *display* a four-digit year value in device-specific windows — such as the Device Status window available from the Hub View or the Bridge View — is dependent on the firmware's ability to *provide* a four-digit value. Not all firmware versions support this ability; contact Cabletron Systems' Global Call Center for information specific to your device firmware.



# Using the FRX4000, FRX6000, and SmartSwitch 1800 Hub View

*Navigating through the Hub View; monitoring hub performance; managing the hub*

---

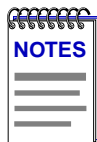
The heart of the SPECTRUM Portable Management Application (SPMA) for the FRX4000, FRX6000, and SmartSwitch 1800 is the Hub View, a graphical interface that gives you access to many of the functions that provide control over the selected FRX or SmartSwitch device and its installed interfaces.

## Using the Hub View

There are two ways to launch the Hub View application: if you are working within a network management system, you can select the **Hub View** option from the icon menu; specific directions for creating an FRX or SmartSwitch icon and accessing the icon menu can be found in the appropriate *Installing and Using...* guide. If you are running the module in a stand-alone mode, type the following at the command line:

```
spmarun frx <IP address> <community name>
```

The community name you use to start the module must have at least **Read** access; for full management functionality, you should use a community name that provides **Read/Write** access. For more information on community names, consult the appropriate hardware documentation.



The *spmarun* script invoked first in the above command temporarily sets the environment variables SPMA needs to operate; be sure to use this command any time you launch an application from the command line. This script is automatically invoked when you launch an application from the icon menu or from within the Hub View.

If there is a hostname mapped to your device's IP address, you can use **<hostname>** in place of **<IP address>** to launch the Hub View. Please note, however, that the hostname is **not** the same as the device name which can be assigned via SPMA; you cannot use the device name in place of the IP address.

Note that the **community name** required to launch the Hub View application (or add the device to your management application or the stand-alone launcher database) is the same as the Node Community Name you must assign when you first configure your device via console management.

## Navigating Through the Hub View

Within the Hub View, you can click mouse buttons in different areas of the window to access various menus and initiate certain management tasks. The following diagrams illustrate the information provided in the Hub View and show you how to use the mouse to display the available menus.

Note that the Hub View display (Figure 2-1, page 2-3) for each device type mimics that device's physical appearance: the FRX4000 and the SmartSwitch 1800 are displayed horizontally, and each contains two "module" slots (one for the LAN interface, and one for the RLP card); the FRX6000 is displayed vertically, and contains eight slots. The type of card (RLP or LAN) installed in each slot, along with its index number, is indicated by the module title box.

For the FRX4000 and the SmartSwitch 1800, whose configurations are fixed, slot 1 will always contain the RLP card; slot 2, the selected LAN interface. Since there's only one of each, each will be indexed 0.

For the FRX6000, RLP indexing is determined by a switch setting on the card itself; RLPs will be displayed in the Hub View in index order, regardless of their actual physical placement in the chassis. LAN cards will also be displayed in index order, after all configured RLPs (again, regardless of actual physical placement in the chassis).

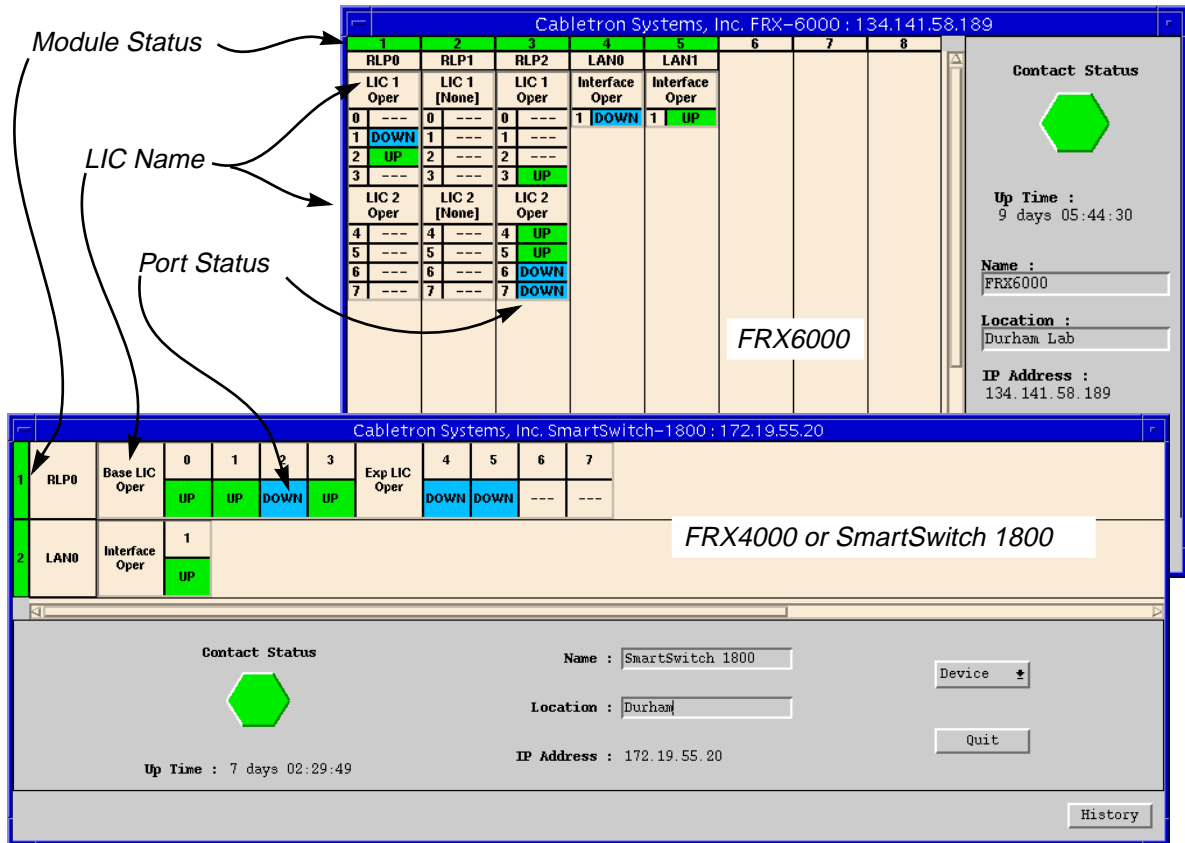
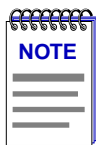


Figure 2-1. The FRX4000, FRX6000 and the SmartSwitch 1800 Hub Views



LAN card indexing is determined simply by the order in which the installed LAN cards are identified during the initial FRX6000 firmware installation. During the firmware installation, you will be prompted to enter the number of LAN cards you have installed, then prompted to supply their type. The order in which you enter the type information determines the indexing.

If you have two cards of the same type, you will need to distinguish them by physical address, as there is no way to control which index is assigned to which card. The physical address is displayed in the LAN Port Information window, described on page 2-23.

Each module display contains individual port boxes that can display a variety of information about each port (see **Selecting a Port Display Form**, page 2-12). For an RLP, up to eight serial ports can be present (four on each of two possible Line Interface Cards, or LICs); for a LAN card, only a single port interface is provided. For the FRX4000 and the SmartSwitch 1800, the Base LIC and Exp (Expansion) LIC correspond to LIC 1 and LIC 2 on each FRX6000 RLP card.

RLP information will only be displayed if the appropriate database record has been configured via console management (see your hardware documentation for more information); for RLPs which have been configured in the database but not yet installed in the chassis, a blue module status will be displayed (see **Port and Module Color Codes**, below). RLPs which are present in the chassis but which have not been configured in the database will not be displayed.

For each configured RLP card, eight serial port status boxes will be displayed (four for each of two possible LIC cards); however, serial port status information will only be displayed for ports which are physically present (on an installed LIC card) and have been configured in the database. Ports which are present but not configured will display a blank status; if no LIC is present, the value [None] will be displayed under the appropriate LIC title, and the associated ports will also display a blank status.

LAN cards will only be displayed when they are both present and configured, as they are configured during the initial firmware installation process, and cannot be configured unless they are present.

### Port and Module Color Codes

Both the module index boxes and the port status boxes are color-coded to indicate status (see [Figure 2-2](#), below).

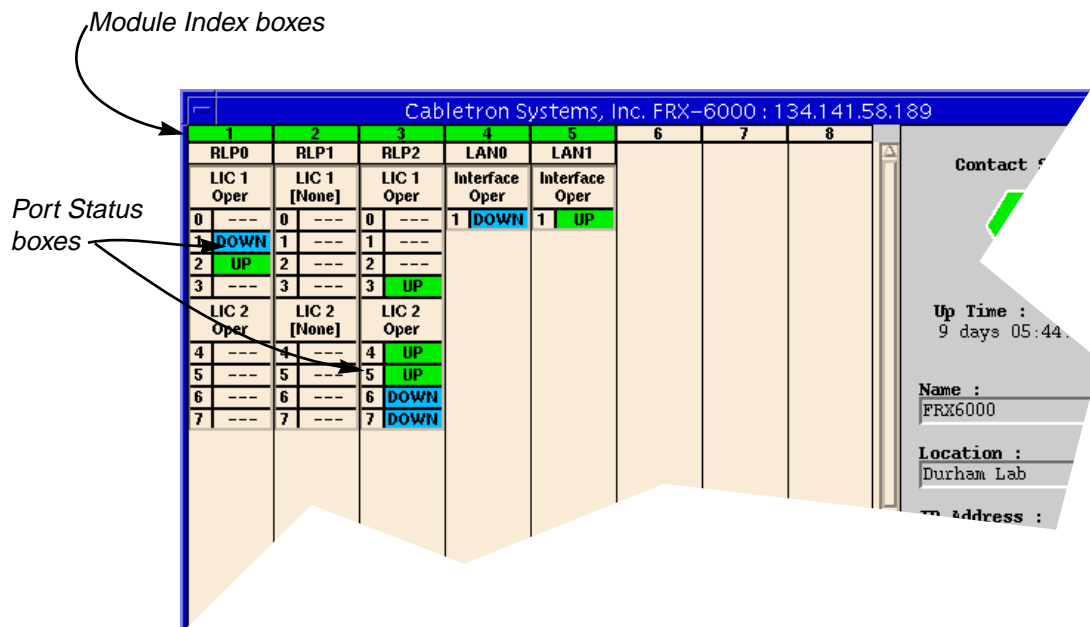


Figure 2-2. Module and Port Color Codes

The module status color code indicates one of two conditions: if a module is both present in the chassis and configured in the database, its index box will be color-coded green; if a module has been configured in the database but is not physically present in the chassis, its index box will be color-coded blue. Modules which are physically present but not yet configured in the database are not displayed at all in the Hub View. (For LAN cards, the module status will always display as green, since they cannot be configured if they are not present.)

The color coding for both serial and LAN ports is based on a combination of MIB II *ifAdminStatus* and *ifOperStatus*, as follows:

Green	indicates that both <i>ifAdminStatus</i> and <i>ifOperStatus</i> are UP.
Blue	indicates that both <i>ifAdminStatus</i> and <i>ifOperStatus</i> are DOWN.
Red	indicates that there is a mismatch in states: one state is UP, and the other is DOWN.
Magenta	indicates that the <i>ifOperStatus</i> is testing, or that the <i>ifOperStatus</i> is DOWN and the <i>ifAdminStatus</i> is testing.
Gray	indicates that the device has returned a value for <i>ifOperStatus</i> which was not understood by SPMA.
Blank	indicates that no response was received from the port. Ports which are not present, or present but not configured in the database, will also display a blank status.

### Using the Mouse in a Hub View Module

For each RLP and LAN card displayed in the Hub View (that is, those which are at least configured in the database), you can use the mouse to access various module- and port-level menus and functions, as illustrated below.

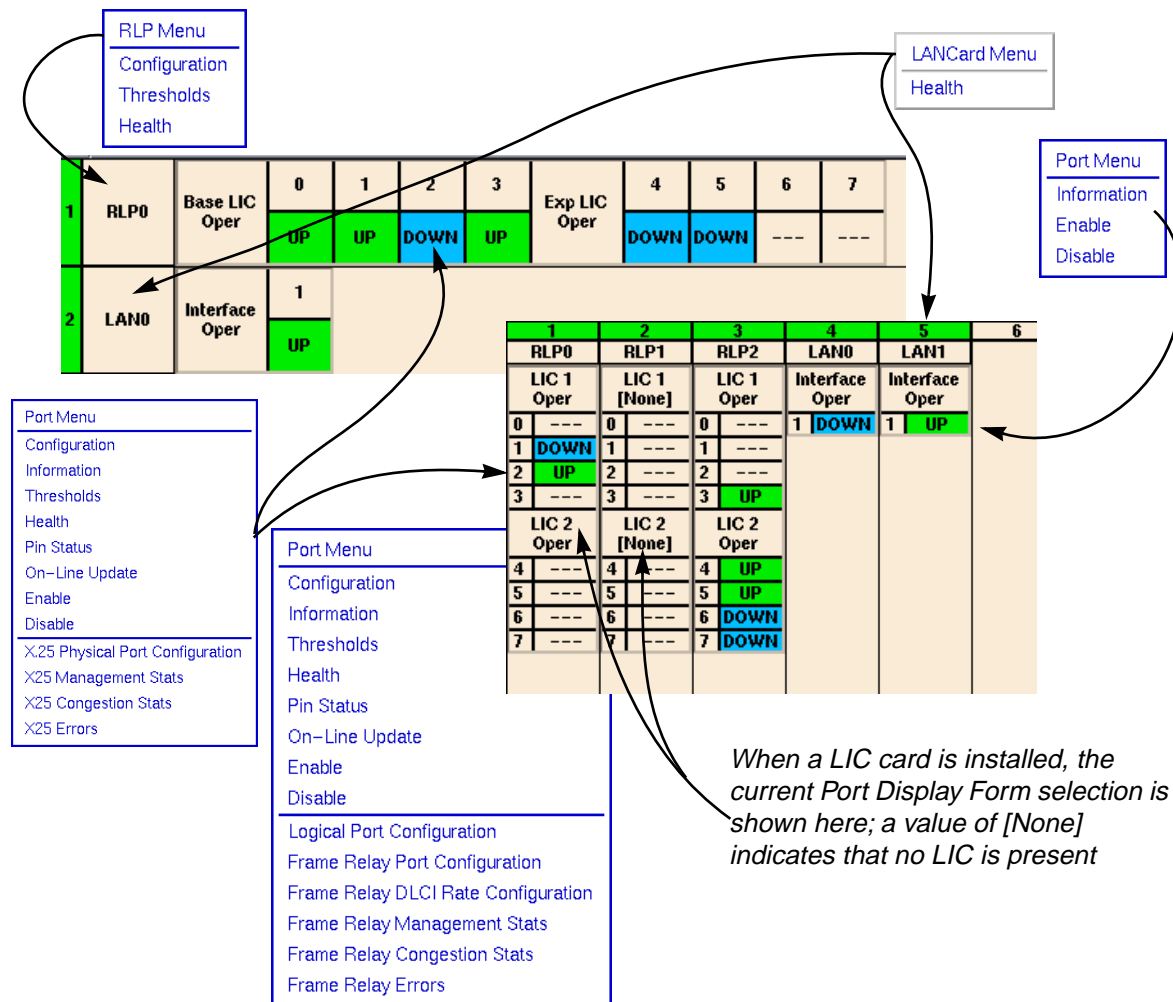


Figure 2-3. Mousing Around a Module Display

## The Hub View Front Panel

In addition to the graphical display of the RLP and LAN cards installed in your device and/or configured in its database, the Hub View gives you device level summary information. The following Front Panel information appears to the right of the module display (for the FRX6000) or below the module display (for the FRX4000 and the SmartSwitch 1800):



**Contact Status** is a color code that shows the status of the connection between SPMA and the device:

- Green means a valid connection.
- Blue means that SPMA is trying to reach the device but doesn't yet know if the connection will be successful.
- Red means that SPMA is unable to contact or has lost contact with the device.

### Uptime

The time that the device has been running without interruption. The counter resets to 00:00:00 (HH:MM:SS) when one of the following occurs:

- Power to the device is cycled.
- The device is reset manually.

### Name

A text field that you can use to help identify the device; you can assign a device name via the MIB I, II application (described in the *SPMA Tools Guide*). To view a name which is longer than the field, click to place your cursor in the text box, and use the arrow keys to shift the display.

### Location

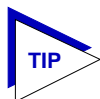
A text field that you can use to help identify the device; you can assign a device location via the MIB I, II application (described in the *SPMA Tools Guide*). To view a location which is longer than the field, click to place your cursor in the text box, and use the arrow keys to shift the display.



*Although you can erase the current **Name** and **Location** values and enter new values in the text fields, you cannot set these values from the Hub View. Any value you attempt to set will remain in the text field only until the Hub View is closed; to permanently change the name or location, you must do so via the MIB I, II application (accessible from the Device menu in the Hub View, from the icon menu, or from the command line). Note that the footer message indicating that the Name or Location field is read-only is in error; these fields are settable, but they cannot be set from the Hub View.*

### IP Address

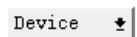
The device's Internet Protocol address; this field will display the IP address you have used to create the device icon (if you are running the Hub View from a management platform) or the IP address you used to launch the Hub View program (if you are running in stand-alone mode). You cannot change the IP address from within SPMA.



*For FRX firmware versions 3.3.0, 3.3.1, and 4.0, each installed LAN card can be assigned an IP address. The IP address you use to communicate with the FRX devices via SNMP is an IP address which has been assigned to a LAN card interface. For FRX6000s which have two LAN cards installed, each can be assigned its own IP address, if desired; either of these IP addresses can be used for SNMP communication.*

*For FRX6000s which do not have a LAN card installed, an IP address can be assigned to any Frame Relay port which is also running the IP protocol; in this case, you would use this IP address to communicate with the device via SNMP and SPMA.*





Clicking the **Device** button displays the Device menu, [Figure 2-4](#).

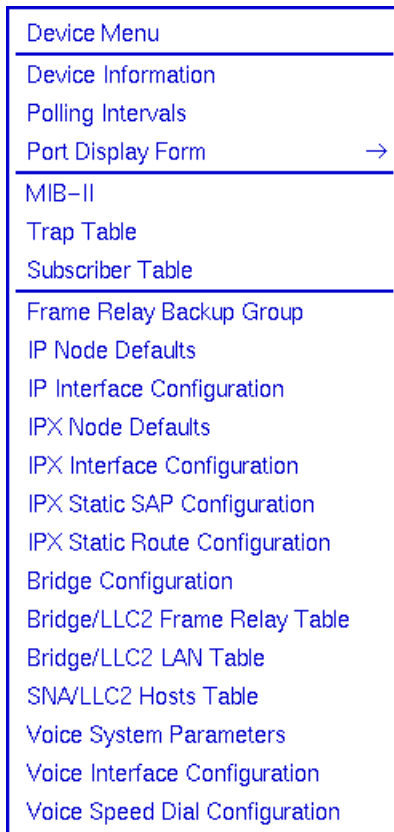


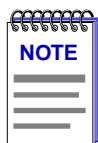
Figure 2-4. Hub View Device Menu

The Device menu lets you perform the following:

- Open the Device Information window (described in **Viewing Device Information**, [page 2-16](#)).
- Open the Polling Intervals window (described beginning on [page 2-32](#)).
- Select a Port Display Form (described beginning on [page 2-12](#)).
- Launch the generic MIB I, II application (described in the *SPMA Tools Guide*).
- Open the Trap Table window (described in Chapter 3, **Configuring the Trap Table**).
- Open the Subscriber Table window (described in Chapter 4, **Configuring the Subscriber Table**).

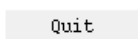
- Open the Frame Relay Backup Group window (described in Chapter 5, **Frame Relay Status and Configuration**).
- Open the IP, IPX, Bridge, and SNA configuration windows (described in Chapters 7, 9, 10 and 11).
- Open the Voice Configuration windows (described in Chapter 12, **Voice Configuration**).

Note that the Device menu does not provide access to all of the applications which are available to the devices; additional applications are available from the Module and Port menus in the Hub View, and some can only be accessed from the icon menu (if you are running under a network management platform) and from the command line (if you are running in stand-alone mode). See Chapter 1, **Introduction to SPMA for the FRX4000, FRX6000, and SmartSwitch 1800**, for a complete list of applications available to the devices and how to access each one.



*Your Device Menu may not display all of the options listed here. Only those protocols and interface types for which your node has been configured will be listed on the menu.*

*Only the SmartSwitch 1800 will display the Voice Configuration options.*



Clicking mouse button 1 on the **Quit** button closes all Hub View application windows; any open applications which can also be accessed from the command line or from the icon menu will remain open.

## Monitoring Hub Performance

The information displayed in the Hub View can give you a quick summary of device activity, status, and configuration. SPMA can also provide further details about hub performance via its three-level menu structure. The Device, Module, and Port menus ([Figure 2-5](#), below) give you control over the hub at three levels and give you access to the tools, menus, and windows that let you monitor specific aspects of hub performance, change hub display options, and set some operating and notification parameters.

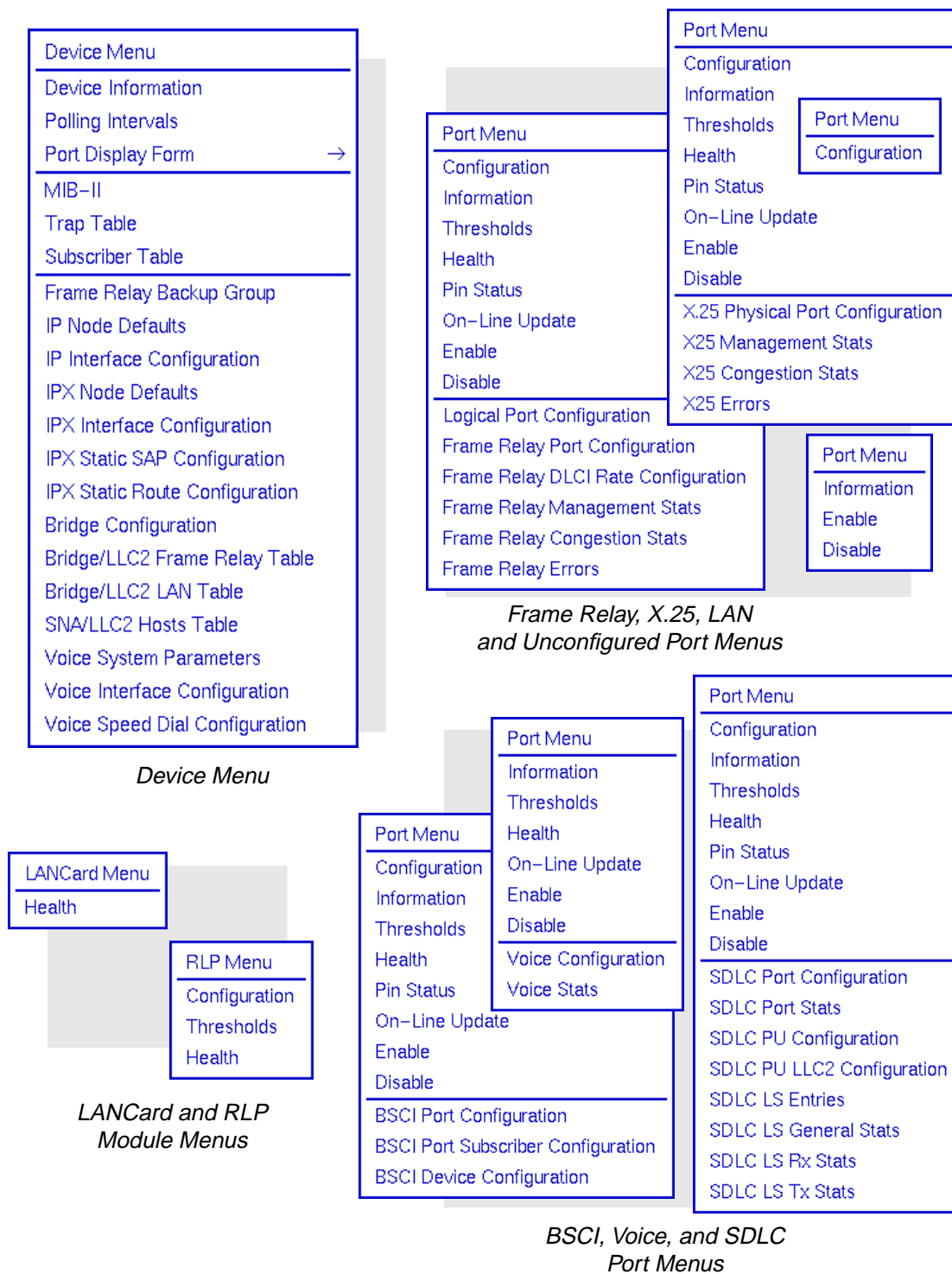
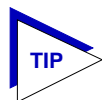


Figure 2-5. The Device, Module, and Port Menus

Hub performance data available through these menus includes:

- Device, Module, and Port configuration information.
- Generic Module and Port health and threshold statistics.
- Serial Port pin status.
- Protocol-specific Port-level statistics.



*The health and protocol statistics are displayed via the SPMA Meters application; for more information on how to manipulate meters, see the **SPMA Tools Guide**.*

## Selecting a Port Display Form

You can change the type of information displayed for each port in the hub by using the Port Display Form options available via the Device menu. Changing the port display form from the Device menu changes the port display for all ports in the chassis.

To change the port display form:

1. Click on the  button to display the Device menu.
2. Drag down to Port Display Form, then to the side as necessary to select one of the port display options. The current selection will be displayed in the LIC name box (for RLPs) or the Interface box (for LAN cards; see [Figure 2-3, page 2-6](#)).

Note that the port color coding does not change based on the selected Port Display Form; see [page 2-4](#) for more information on color codes.

Port display forms are:

### Operation Status

The Operation Status port display form indicates the current value of the *ifOperStatus* OID:

UP	operational status up
DOWN	operational status down
TEST	operational status testing
UNK	unknown; device is returning a value that the software does not recognize
---	the device is not responding to the request

**Admin Status**

The Admin Status port display form indicates the current value of the *ifAdminStatus* OID:

UP	the port has been administratively enabled
DOWN	the port has been administratively disabled
TEST	the port has been administratively placed in a test mode
UNK	unknown; device is returning a value that the software does not recognize
---	the device is not responding.

**Port Type**

The Port Type port display form indicates the type of protocol the selected port has been configured to run, as defined by the OID *nIfType*. Possible values for any one port are limited to the protocols that have been installed on that port's RLP card:

X25	indicates that the port has been configured to run the X.25 protocol -- either <i>ddnX25</i> or <i>rfc877x25</i> .
sdlc	indicates that the port has been configured to run the SDLC protocol.
frame	indicates that the port has been configured to run the Frame Relay protocol.
async	indicates that the port has been configured to run the asynchronous protocol.
bsci	indicates that the port has been configured to run the bi-synchronous (two-directional) protocol.
ether (LAN only)	indicates that the port is supporting an Ethernet connection: either <i>ethernetCsmacd</i> , or <i>iso88023Csmacd</i> .
tr (LAN only)	indicates that the port is supporting a Token Ring connection.
voice	indicates that the port is supporting a voice connection.

**Port State**

The Port State display indicates the port's readiness (or lack thereof) to establish a connection and transmit data (as defined by the OID *nIfPortStatus*):

linkup	A physical electrical connection is present and working (cable is connected at both ends and the two connected ports are communicating), but some configuration information is missing or there is a line speed or other mismatch. This state is one step short of operational.
oper (operational)	The port is functional and capable of data transmission.

disa (disabled)	The port is operationally disabled.
disc (disconnect)	One of the two endpoints connected via the port has closed the connection.
conf (configured)	The port has been configured in the database, but the configured protocol has not been installed on the associated RLP card.
dial (dialReady)	For a frame relay port, this state indicates that the port has been configured as a backup port, and it is ready to be switched into use if needed; for an X.25 port, this state indicates that the port is ready to transmit or receive calls.
quies (quiesced)	A port which has been quiesced will be disabled when all active calls have been completed. No new calls can be initiated during this delayed disable state. Once a quiesced port is disabled, it will remain disabled until it is enabled by management action.
fail (failed)	The port has failed due to a broken cable or other wire problem, either while moving to the operational state or after achieving it.
fault (hardware fault)	Indicates that the port has failed due to a hardware problem on the serial port itself.
na	Not applicable; this value displays for any LAN ports installed in the device.
other	The port status response received from the device was not understood by SPMA.
ipl	The port is in a booting state (initial program load). This is a very brief transitional state that is unlikely to be displayed.
restar (restarting)	A very brief transitional state that occurs during boot up; this state is unlikely to be displayed.
onhook	Indicates there is no call in progress and the voice port is able to accept an incoming call.
offhook	Indicates there is a call in progress and the voice port is not able to accept an incoming call.
dialing	Indicates a call is being placed but has not been accepted yet.
active	Indicates a call has been placed and answered.
pending	The device at the remote end has been placed onhook while the call was still in progress.

**Connector Type**

This port display form indicates the connector type supported by the selected port. This value (from the OID *nIfConnectorType*) is determined by a combination of cable and physical port type, as follows:

rs232	Indicates an RS232 serial port, which must always use an RS232 cable.
v35	Indicates a v.35 serial port, which must always use a v.35 cable.
rs449	Indicates an RS422 serial port configured for an RS449 cable.
rs530	Indicates an RS422 serial port configured for an RS530 cable.
x21	Indicates an RS422 serial port configured for an X21 cable.
csudsu (csu/dsu)	Indicates a CSU/DSU interface.
none	This value displays for LAN ports.
voice	This value displays for voice channels.

**Speed**

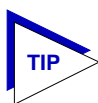
Indicates the speed configured for the selected port, as reported by the MIB II OID *ifSpeed*. The speed configured for a port must match the speed of the line which will be connected to that interface, and the speed configured for the port at the other end of the connection.

**Max Packet Size**

Displays the size of largest datagram which can be sent or received on this port, in octets (as reported by the MIB II OID *ifMtu*). This value is specific to the protocol running on the selected interface.

**IF Index**

Displays the MIB II *ifIndex* value assigned to each port. Note that the displayed index values do not necessarily increment as you might expect — as the FRX or SmartSwitch 1800 device boots, each physical or *logical* port which is detected will be incrementally assigned an index value, which may result in gaps between the index values assigned to the physical ports displayed in the Hub View. Note that the assigned *ifIndex* values are constant between bootups; however, once the device reboots, the same *ifIndex* values will not necessarily be assigned to the same physical or logical ports (if the device's configuration has changed).



To map logical ports to their physical port locations, use the OID *nIfPhyPort*.

## Viewing Device Information

The Device Information window provides some general descriptive information about the FRX or SmartSwitch 1800 device you are modeling.

To access the window:

1. In the Hub View, click on  to display the Device menu.
2. Drag down to **Device Information**, and release. The Device Information window, [Figure 2-6](#), will appear.



Figure 2-6. The Device Information Window

Device information includes:

System Description	Displays the MIB II <i>sysDescr</i> for the selected device; this description typically includes information about the firmware version currently running.
System Contact	Displays the MIB II <i>sysContact</i> value; this value is settable via the generic MIB I, II application (accessible from the Device menu, the icon menu, or from the command line). See the <i>SPMA Tools Guide</i> for a detailed description of the MIB I, II application and how to set this value.

## Configuring RLP Protocols

The RLP Configuration window provides information about the status of each displayed RLP and lets you view and configure the protocols loaded onto the selected RLP.

To access the window:

1. In the Hub View, click on the appropriate Module Index or Module Name text box to display the RLP Menu (see [Figure 2-3](#), [page 2-6](#)).
2. Drag down to **Configuration**, and release. The RLP Configuration window, [Figure 2-7](#), will appear.



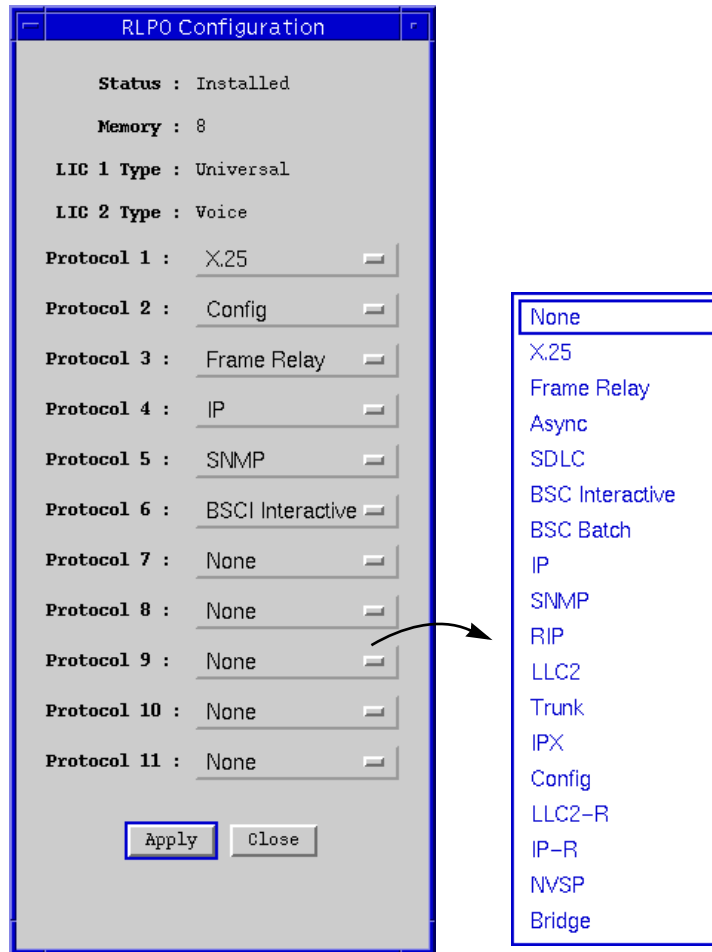
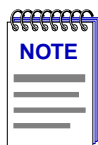


Figure 2-7. The RLP Configuration Window and Protocol Menu

RLP status information includes:

- |        |   |
|--------|---|
| Status | A status of <b>Installed</b> indicates that the RLP is physically present in the chassis, and has been configured in the database; a status of <b>Configured</b> indicates that a database record has been configured, but the card is not physically present in the hub. |
| Memory | Displays the amount of memory installed on the selected RLP, either 4 or 8 megabytes.   |



You must have 8 megabytes of memory installed on at least one RLP in the FRX to run firmware version 4.0. If you have RLPs with only 4 megabytes of memory and want to upgrade them to 8 megabytes, contact Cabletron's Global Call Center or your local service representative for more information.

**LIC 1 Type/LIC 2 Type** Displays the type value for each Line Interface Card (LIC) installed on the selected RLP: RS232, HS RS232, v.35, RS422, Voice or Universal. The Universal LIC is shipped as the Base LIC on the FRX4000 and the SmartSwitch 1800. It has four ports: port 0 can be configured for RS232 operation; port 1 can be configured for RS232 and CSU/DSU operation; ports 2 and 3 can be configured for RS232, v.35, RS449, RS530, or x.21 operation (depending on the attached cable type).

**Protocols** Displays the protocols that have been loaded onto the selected RLP. On the FRX4000 and SmartSwitch 1800, a maximum of 11 protocols can be loaded on to RLP0. A maximum of nine protocols can be loaded on to an FRX 6000 RLP. If less than the maximum number have been loaded, some of the protocol fields will display **None**. Only protocols which have been loaded onto the RLP can be configured to run over that RLP's serial ports. You can change or add protocols for the selected RLP.



For the FRX4000 and the SmartSwitch 1800, the RLP Configuration window and protocol menu will display all the protocols shown in [Figure 2-7](#), but only those protocols that were purchased will be configurable.

For the FRX6000, all supported protocols will fit on one 8-megabyte RLP; however, it is recommended that no more than seven protocols be configured on any one RLP.



The X.25 protocol is always loaded on every RLP; it is a necessary protocol for use by internal FRX and SmartSwitch 1800 traffic and **must not** be deleted.

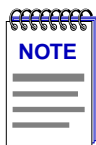
Follow these guidelines when configuring protocols:

- RIP is a valid choice only if IP is already configured on the same RLP.
- If SNMP is configured, IP must also be configured. For the FRX6000, SNMP and IP can be, but do not have to be, on the same RLP.

- If LLC2 is configured, Bridge must also be configured. For the FRX6000, both protocols should be, but do not have to be, on the same RLP. Having them on the same RLP should provide better performance.
- If NVSP is configured, LLC2 and Bridge must also be configured. For the FRX6000, all three protocols can be, but do not have to be, on the same RLP.
- For the FRX6000, IP, SNMP, RIP, IPX, LLC2, NVSP, and Bridge cannot be configured on more than one RLP each. However, more than one of these can be on the same RLP. Performance can be enhanced by configuring these protocols on the same RLPs that contain the frame relay ports that will transport the protocols.

To change or add protocols for the selected RLP:

1. Display the Configuration window for the selected RLP. Each protocol field will display either a configured protocol or **None**.
2. To change a protocol, click on the menu button to display a list of options, then drag up or down to select the option you want.
3. Click on **Apply** to save your changes.



*Changing the protocols in the RLP Configuration window will enable the protocols on that RLP, but to make the protocols actually operational you must reboot the device.*

## Configuring Serial Port Protocols

The Port Configuration window lets you configure a protocol for the selected port.

To access the window:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Configuration**, and release. The Port Configuration window, [Figure 2-9](#), will appear.

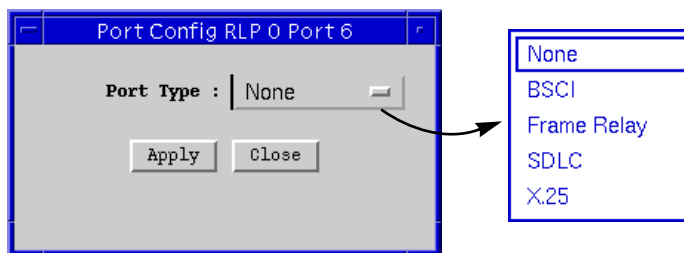


Figure 2-8. The Port Configuration Window and Protocol Menu

To change or add a protocol for the selected port:

1. Display the Configuration window for the selected port. It will display either a configured protocol or **None**.
2. To change a protocol, click on the menu button to display a list of options, then drag up or down to select the option you want. The Protocol menu will only list protocols that are supported on that RLP.
3. Click on **Apply** to save your changes.

## Viewing Serial Port Information

The Port Information windows provide the same descriptive information for all displayed serial ports, regardless of type. Note that this information is only available for serial ports which are both configured in the database and physically present in the chassis.

To access serial port information:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Information**, and release. The Port Info window, [Figure 2-9](#), will appear.

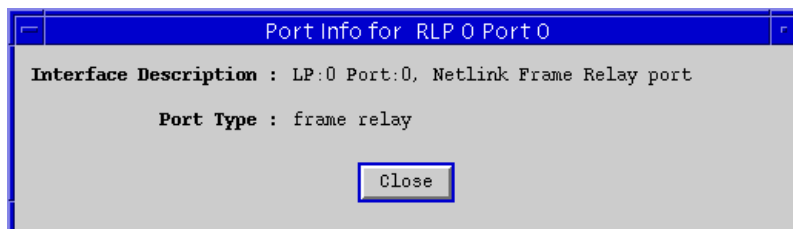


Figure 2-9. The Serial Port Information Window

**Interface Description:** Displays a general description of the selected serial interface (from the MIB II *ifDescr*), including the index number assigned to the port's RLP; the physical number assigned to the port interface itself (as designated in the Port Index box in the Hub View), and a general text description of the port, including the protocol currently configured to run over that port.

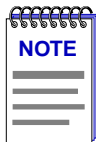


*Note that the index number assigned to the physical port interface is **not** the same as the ifIndex assigned to that same physical interface. The physical port indices begin with 0; the ifIndex values begin at 1.*

**Port Type:** Displays the type of protocol the selected port has been configured to run, as defined by the OID *nIfType*. Note that this is the same information displayed by the Port Type port display form (described on [page 2-13](#)).

### Serial Port Pin Status

You can also view the electrical status of each pin on the cables attached to a serial port; this information can be useful in tracking down connectivity problems, especially those related to cable failure.



*The current version of firmware for the SmartSwitch 1800 does not support the Serial Port Pin Status function on its two voice ports.*

To view serial port pin status:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Pin Status**, and release. The Pin Status window, [Figure 2-10](#), will appear.

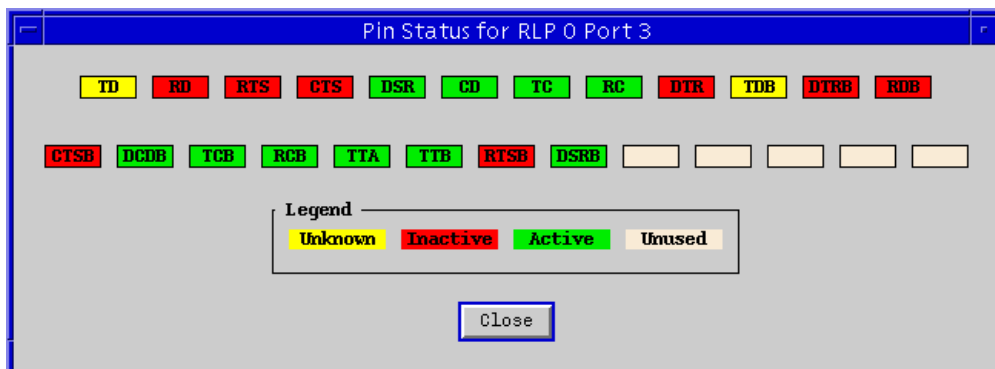
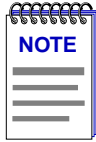


Figure 2-10. The Pin Status Window

Each cable pin is represented by a colored rectangle labeled with the pin name; the color-coding tells you whether the pin is active (green; has voltage), inactive (red; has no voltage), unused (tan, or no color), or its electrical status is unknown (yellow). Each serial port provides information about the following pins:

TD (transmit data)	Pin will be active when the connection is operational.
RD (receive data)	Pin will be active when the connection is operational.
RTS (request to send)	For some protocols, the pin will become active when the device wishes to send some data, and become inactive once the data is sent; for a point-to-point protocol, however, the pin will always be active.
CTS (clear to send)	The receiving device has responded to a request to send.
DSR (data set ready)	When active, indicates that the remote data communications equipment (DCE) has signalled that it is ready.
CD (carrier detect)	When active, indicates that the connected line is operational (that is, a dial tone or similar indication is present).
TC (transmit clocking)	When active, indicates that clocking is occurring on the link.
RC (receive clocking)	When active, indicates that clocking is occurring on the link.
DTR (data terminal ready)	When active, indicates that the data terminal equipment (DTE) is ready.
TTA (transmit timing)	When active, indicates that timing frames are being transmitted.



The pin names which end in “B” — TDB, RDB, CTSB, DCDB, TCB, RCB, TTB, RTSB, and DSRB — have the same definitions as those listed above, but for the B channel signals used by V.35 and RS449 interfaces.

## Viewing LAN Port Information

The LAN Port Information windows also provide general descriptive information about the selected port. To access LAN port information:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Information**, and release. The Port Info window, [Figure 2-11](#), will appear.

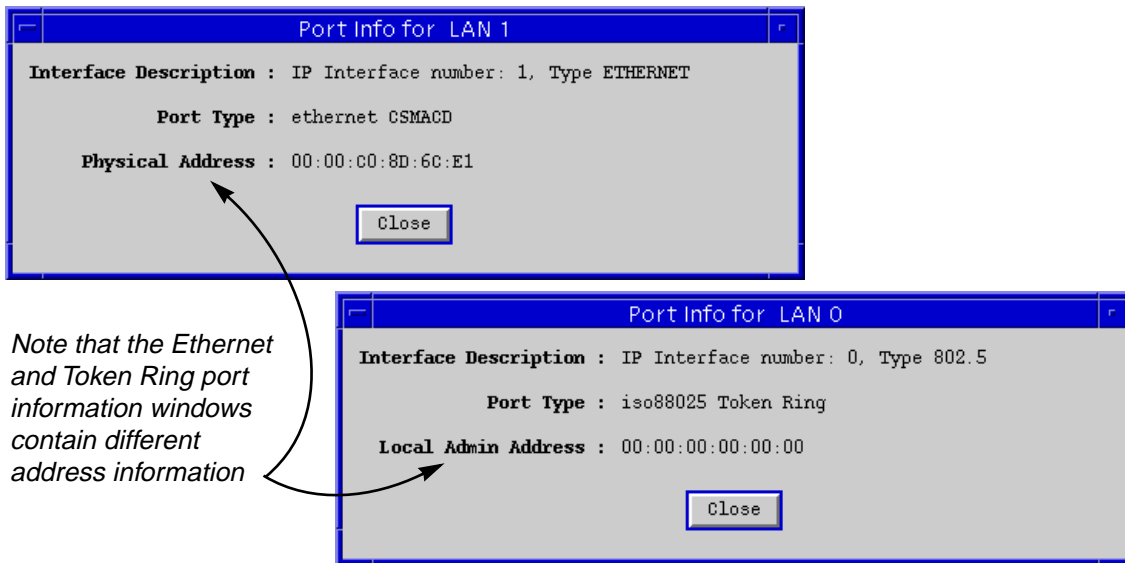
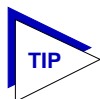


Figure 2-11. LAN Port Information Windows

The windows display the following information:

- Interface Description: Displays a general description of the selected LAN interface (from the MIB II *ifDescr*), including the index number assigned to the port’s LAN card (0 or 1), and a general text description of the port (802.5 or Ethernet).
- Port Type: Displays the LAN port type: iso88025 Token Ring, or ethernet CSMACD.

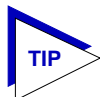
Address: For Token Ring LAN cards, this field displays the locally administered physical address, if one has been assigned; if none has been assigned, the field (labeled **Local Admin Address**) will display all zeros. For Ethernet cards, the factory-set physical address (labeled **Physical Address**) will be displayed.



*For an FRX6000 with two LAN cards of the same type, note that the only way to distinguish between the two cards is via the physical address displayed here (since indexing is unrelated to physical position in the chassis).*

## Viewing Statistics

The Hub View can provide a variety of statistics at the RLP, serial port, and LAN card levels that give you an overview of the general health of your network connections. These statistics are described in the following sections.



*The statistics windows provided via the Hub View display data using the SPMA Meters application; for more information on how to manipulate the meter display and change meter settings, see the **SPMA Tools Guide**.*

## RLP Health

To access RLP Health statistics:

1. In the Hub View, click on the appropriate Module Index or Module Name text box to display the RLP Menu (see [Figure 2-3](#), [page 2-6](#)).
2. Drag down to **Health**, and release. The RLP Health Statistics window, [Figure 2-12](#), will appear.



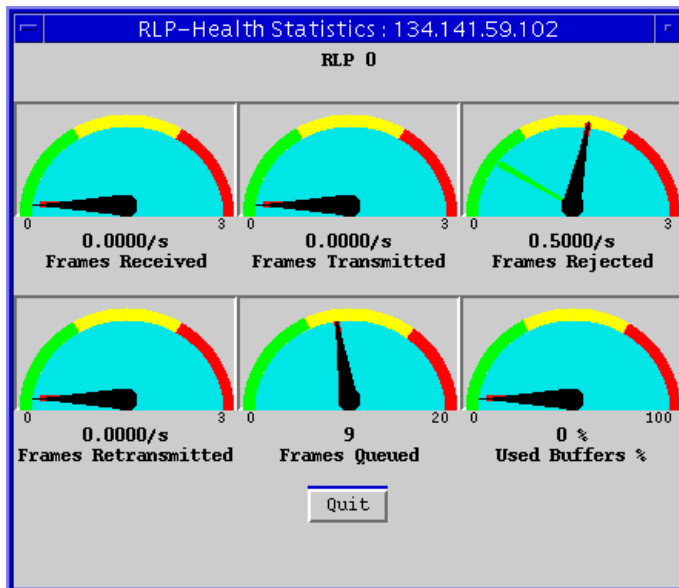


Figure 2-12. The RLP Health Statistics Window

RLP Health statistics provide the following general usage information for all ports on the selected card:

- |                      |  |
|----------------------|--|
| Frames Received      | The total number of frames received on all active serial ports on the selected RLP, expressed as a rate (frames/second).   |
| Frames Transmitted   | The total number of frames transmitted by all active serial ports on the selected RLP, expressed as a rate (frames/second).  |
| Frames Rejected      | The total number of frames rejected by all active serial ports on the selected RLP, expressed as a rate (frames/second). Each protocol handles rejected frames a little differently; in general, however, frames are rejected because the active protocol has detected an error in the frame itself.   |
| Frames Retransmitted | The total number of frames retransmitted by all active serial ports on the selected RLP, expressed as a rate (frames/second). Frames are typically retransmitted to correct errors or if the receiving device was too busy to receive the original frames; a high retransmit rate can indicate a noisy transmission line. If this value is consistently above zero and there are no other problems, you may want to increase the value assigned to the Retransmission Timer in the port database record. (See your hardware documentation for more information.) |

Frames Queued	The total number of frames from all active serial ports on the selected RLP currently queued and waiting for transmission, expressed as a raw value. Queued frames will be transmitted as soon as device resources permit.
Used Buffers	Displays the percentage of available buffers currently being used by queued frames.

## Serial Port Health

To access Serial Port Health statistics:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Health**, and release. The Port Health Statistics window, [Figure 2-13](#), will appear.

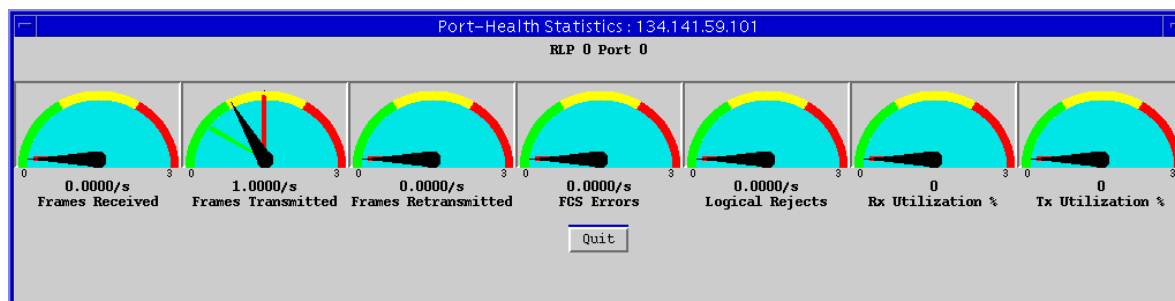


Figure 2-13. The Port Health Statistics Window

The Serial Port Health Statistics windows display the same statistics for each configured serial port, regardless of type:

Frames Received	The total number of frames received on the selected serial port, expressed as a rate (frames/second).
Frames Transmitted	The total number of frames transmitted on the selected serial port, expressed as a rate (frames/second).
Frames Retransmitted	The total number of frames retransmitted on the selected serial port, expressed as a rate (frames/second). Frames are typically retransmitted to correct errors or if the receiving device was too busy to receive the original frames; a high retransmit rate can indicate a noisy transmission line.
FCS Errors	The total number of frames received at the selected serial port that contained a bad frame check sequence (FCS), expressed as a rate (errors/second). The frame check

sequence (like the CRC, or cyclic redundancy check) is a value computed at both the sending and receiving ends of the connection; if the computed values don't match, the frame is assumed to have been corrupted in transit. A value consistently greater than zero indicates line problems.

Logical Rejects	The sum of <i>frame rejects</i> — frames which are dropped due to congestion or some other transmission problem — and <i>reject frames</i> — protocol frames that notify the sender that one or more packets is missing from a sequence. The total is expressed as a rate (rejects/second); a value consistently greater than zero indicates line problems.
Rx Utilization %	The ratio of non-flag characters (the space between frames) to the total number of characters received on the selected serial port; that is, the percentage of available bandwidth being utilized.
Tx Utilization %	The ratio of non-flag characters (the space between frames) to the total number of characters transmitted on the selected serial port; that is, the percentage of available bandwidth being utilized.

## LAN Card Health

The LAN Card Health Statistics window provides standard MIB II stats for the selected LAN interface; note that the same statistics are provided for both Ethernet and Token Ring interfaces.

To access LAN Card Health statistics:

1. In the Hub View, click on the appropriate Module Index or Module Name text box to display the LANCard Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Health**, and release. The LAN Health Statistics window, [Figure 2-14](#), will appear.

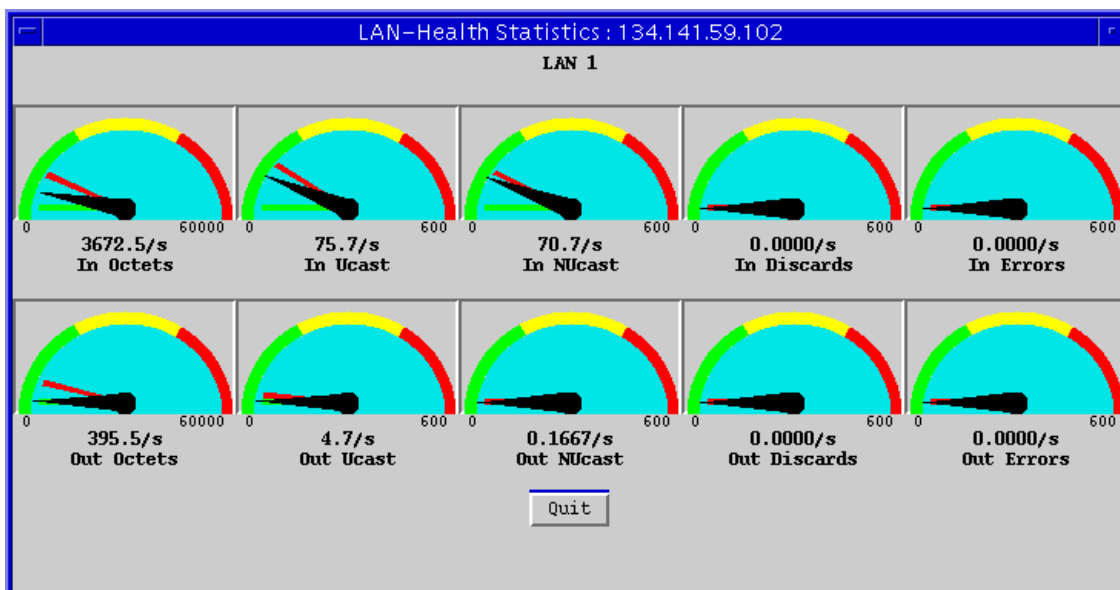


Figure 2-14. The LAN Health Statistics Window

MIB II statistics provided are:

In Octets	<i>(ifInOctets)</i> The total number of octets (or bytes) of data received at the selected LAN interface, expressed as a rate (octets/second).
In Ucast	<i>(ifInUcastPkts)</i> The total number of packets received at the selected LAN interface that were destined for a single address (unicast), expressed as a rate (packets/second).
In NUCast	<i>(ifInNUcastPkts)</i> The total number of packets received at the selected LAN interface that were destined for more than one address (either broadcast or multicast), expressed as a rate (packets/second).
In Discards	<i>(ifInDiscards)</i> The total number of inbound packets which were discarded even though no errors were detected, expressed as a rate (packets/second); well-formed packets are typically discarded in order to free up buffer space.
In Errors	<i>(ifInErrors)</i> The total number of inbound packets which contained errors that prevented them from being delivered, expressed as a rate (packets/second).
Out Octets	<i>(ifOutOctets)</i> The total number of octets (or bytes) of data transmitted by the selected LAN interface, expressed as a rate (octets/second).

Out Ucast	<i>(ifOutUcastPkts)</i> The total number of packets transmitted by the selected LAN interface that were destined for a single address (unicast), expressed as a rate (packets/second).
Out NUcast	<i>(ifOutNUcastPkts)</i> The total number of packets transmitted by the selected LAN interface that were destined for more than one address (either broadcast or multicast), expressed as a rate (packets/second).
Out Discards	<i>(ifOutDiscards)</i> The total number of outbound packets which were discarded even though no errors were detected, expressed as a rate (packets/second); well-formed packets are typically discarded in order to free up buffer space.
Out Errors	<i>(ifOutErrors)</i> The total number of outbound packets which contained errors that prevented them from being delivered, expressed as a rate (packets/second).

## Viewing Statistics Thresholds

The Hub View provides a way to view trap thresholds that have been set through console management for RLP and port health statistics. For each RLP and port statistic, you can specify a threshold that, when crossed, causes a trap to be sent to a management workstation. A threshold is either a number or a percentage, depending on the statistic. The valid range for any number threshold is 0 - 65535 with the default value being 0. When the measured value for the health statistic crosses the threshold (in either direction), a trap is sent to the collecting management workstation. (For information on designating workstations to accept traps, see Chapter 3, **Configuring the Trap Table**. For definitions of RLP and Serial Port Health Statistics, see **Viewing Statistics**, page 2-24.)

### RLP Statistics Thresholds

To view RLP Thresholds:

1. In the Hub View, click on the appropriate Module Index or Module Name text box to display the RLP Menu (see **Figure 2-3**, page 2-6).
2. Drag down to **Thresholds**, and release. The RLP Statistics Thresholds window, **Figure 2-15**, will appear.

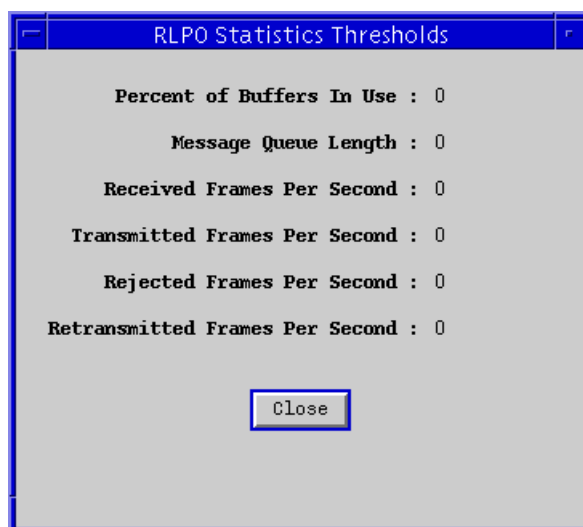


Figure 2-15. The RLP Statistics Thresholds Window

The RLP Statistics Thresholds window shows the current threshold value (either a number or a percentage) for the following RLP health statistics (for definitions of the RLP Health Statistics, see [RLP Health, page 2-24](#)):

Percentage of Buffers in Use	Shows the threshold for the Used Buffers statistic.
Message Queue Length	Shows the threshold for the Frames Queued statistic.
Received Frames Per Second	Shows the threshold for the Frames Received Statistic.
Transmitted Frames Per Second	Shows the threshold for the Frames Transmitted Statistic.
Rejected Frames Per Second	Shows the threshold for the Frames Rejected statistic.
Retransmitted Frames Per Second	Shows the threshold for the Frames Retransmitted statistic.

### Serial Port Statistics Thresholds

To view Serial Port Thresholds:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).

2. Drag down to **Thresholds**, and release. The Port Statistics Thresholds window, [Figure 2-16](#), will appear.

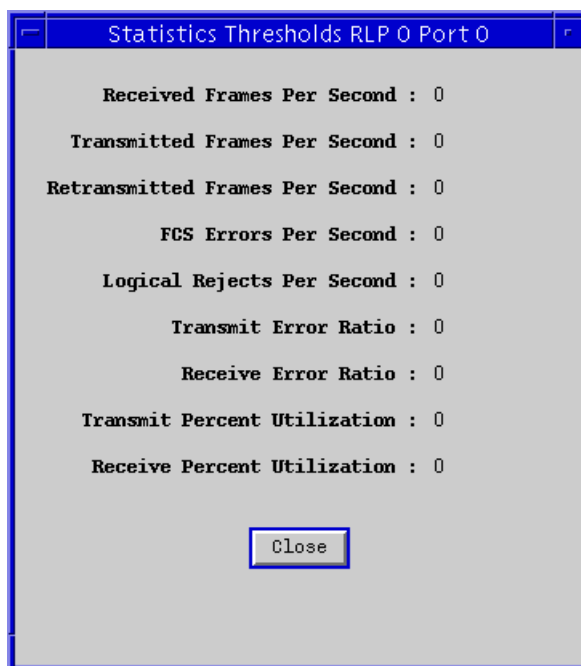


Figure 2-16. The Port Statistics Thresholds Window

The Port Statistics Thresholds window shows the current threshold value (either a number or a percentage) for the following Port health statistics (for definitions of the Port Health Statistics, see [Serial Port Health](#), page 2-26):

Received Frames Per Second	Shows the threshold for the Frames Received statistic.
Transmitted Frames Per Second	Shows the threshold for the Frames Transmitted statistic.
Retransmitted Frames Per Second	Shows the threshold for the Frames Retransmitted statistic.
FCS Errors Per Second	Shows the threshold for the FCS Errors statistic.
Logical Rejects Per Second	Shows the threshold for the Logical Rejects statistic.
Transmit Error Ratio	Shows the threshold for the Transmit Error Ratio statistic. This statistic is the ratio of retransmitted frames per second to successfully transmitted frames per second on the port.

Receive Error Ratio	Shows the threshold for the Receive Error Ratio statistic. This statistic is the ratio of frames rejected per second to frames accepted per second on the port.
Transmit Percent Utilization	Shows the threshold for the Tx Utilization % statistic.
Receive Percent Utilization	Shows the threshold for the Rx Utilization % statistic.

## Managing the Hub

In addition to the performance information described in the preceding sections, the Hub View also provides you with the tools you need to configure your device and keep it operating properly. Hub management functions include setting the polling intervals, and enabling and disabling serial ports.

### Setting the Polling Intervals

To set the polling intervals used by SPMA and the FRX:

1. Click on **Device** to display the Device menu.
2. Drag down to **Polling Intervals**, and release.

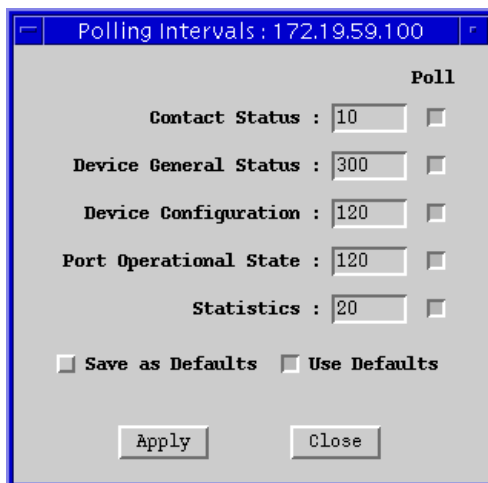




Figure 2-17. FRX Hub View Polling Intervals

3. To activate the desired polling, click mouse button 1 on the selection box to the right of each polling type field.



4. To change a polling interval, highlight the value you would like to change, and enter a new value in seconds. Note that the **Use Defaults** option must *not* be selected, or values will revert back to default levels when you click on  , and your changes will be ignored.
5. If you wish to use your new polling interval settings as the default values that SPMA will use for each FRX or SmartSwitch 1800 you are managing, use mouse button 1 to select the **Save As Defaults** option.
6. If you wish to replace existing values with the current set of default values, use mouse button 1 to select the **Use Defaults** option.
7. Click mouse button 1 on  once your changes are complete. Changes take effect after the current polling cycle is complete.

You can set the update intervals for the following:

#### **Contact Status**

This polling interval controls how often the FRX or SmartSwitch 1800 is “pinged” to check SPMA’s ability to maintain a connection with the device.

#### **Device General Status**

This polling interval controls how often the Hub View Front Panel Information — such as Uptime, Device Name, and so forth — and some status information is updated.

#### **Device Configuration**

This polling interval controls how often a survey is conducted of the type of equipment installed in the FRX or SmartSwitch 1800; information from this poll would change the Hub View to reflect the addition and/or removal of an RLP or LAN card.

#### **Port Operational State**

This polling interval controls the update of the information displayed in the Port Status boxes for each port in the hub. Port state information varies according to the Port Display Form which is currently selected.

#### **Statistics**

This polling interval controls how often the information displayed in the Port Status boxes is updated when the Port Display Form is set to a rate or percentage.



*SPMA generates network traffic when it retrieves the above-described information; keep in mind that shorter intervals mean increased network traffic. Range limits for these polling times are 0-999,999 seconds; however, an entry of 0 will be treated as a 1.*

## Enabling and Disabling Serial Ports

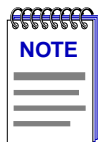
You can use the Port Menu available for each configured serial port and LAN port to change the selected port's administrative status. To do so:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **Enable** or **Disable**, as desired, and release.

## Applying Port-level Changes

After you have made any port-level configuration changes (such as configuring an SNA or BSCI port), your changes will not take effect until you have done an on-line update. To do so:

1. In the Hub View, click on the appropriate Port Index or Port Status text box to display the Port Menu (see [Figure 2-3, page 2-6](#)).
2. Drag down to **On-line Update** and release.



*After you have made system-level changes (such as configuring an IP Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

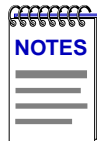
# Configuring the Trap Table

*A few words about traps; accessing the Trap Table window; configuring the trap table*

---

## About Traps

The FRX4000, FRX6000, and the SmartSwitch 1800 have the ability to issue unsolicited SNMP traps to notify management stations of unusual events. These traps will not be issued, however, until the device's trap table has been properly configured, designating one or more workstations to receive the traps and selecting the traps that will be sent. This configuration can be performed via the Trap Table.



*SPMA does not accept the trap messages; that task is left to your network management platform. (See the appropriate network management system documentation for details about viewing trap messages.) If you are using SPMA in a stand-alone mode, traps directed to a workstation which does not have some facility for accepting them will be ignored.*

*In addition, so that your network management platform can interpret the FRX trap messages, you must have properly installed and configured the Cabletron trap file included with your software. This process should have occurred during installation; see your **Installing and Using...** guide for details.*

## Launching the Trap Table

To launch the Trap Table:


1. Click on the **Device**  button to display the Device menu.
2. Drag down to **Trap Table**, and release. The Trap Table window, [Figure 3-1](#), will appear.



Figure 3-1. The Trap Table

The list box at the top of the window displays the trap table entries that have already been configured; the fields and buttons in the lower portion of the window allow you to add new entries and modify or delete existing ones. Each device can support up to 16 entries in its trap table.

Each trap table entry contains the following parameters:

**IP Address**

Indicates the IP address of the management workstation that will receive traps. Be sure this is a management workstation which has some facility for accepting and displaying traps, or traps sent there will be ignored.

**Status**

Each trap table entry can be either enabled or disabled; when enabled, the entry is active and the designated traps will be sent when they occur. No traps are sent to disabled entries.

**Severity**

Each trap issued by the FRX or SmartSwitch 1800 contains a severity designation, indicating the importance of the event it is announcing; you can use these levels to filter the traps you wish to send to each designated workstation. Only those

traps with a severity level equal to or greater than this severity setting will be forwarded to the associated management workstation. Each trap is assigned one of four severity levels:

Informational	Indicates an informational event (no action generally required) or a small configuration error. This is a Level 4 severity.
Minor	Indicates a minor fault or traffic disturbance; recommended action typically involves clearing the fault at the first suitable occasion. This is a Level 3 severity.
Major	Indicates a major fault or link alarm; corrective action should be taken as soon as possible. This is a Level 2 severity.
Critical	Indicates a serious fault or error that requires immediate action. This is a Level 1 severity.

## Configuring Traps

To add a trap table entry:

1. In the **IP Address** field, enter the IP address of the workstation to which you wish to direct trap messages from the selected FRX or SmartSwitch 1800 device. Be sure this is a workstation with some facility for accepting and displaying SNMP traps.
2. In the **Status** field, click to either enable or disable your new entry. If you disable an entry, no traps will be sent to its designated workstation.
3. Use the **Severity Level** field to select which traps you wish to send to the selected workstation: only those traps with severity levels equal to or exceeding the level assigned here will be forwarded to the selected workstation.
4. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the entry you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the **IP Address**, **Status**, and/or **Severity Level** fields, as desired.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the entry you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.

## Trap Messages

Following are some general descriptions of traps that may be sent by your FRX or SmartSwitch 1800 device, including the conditions or events they announce, the level of severity assigned to those conditions or events, the numeric designation assigned to the trap, and, where appropriate, suggestions for corrective action.

### **Transmitter Stuck** **146**

No clock is being generated.

*Severity*            Informational (Level 4)

*Action*             Check configurations and set the clock.

### **Configured for extended sequence numbering, received SABM** **181**

The Port record is configured for a maximum frame sequence number (Outstanding Frames) greater than seven, but a command was received setting the mode to allow a maximum of seven.

*Severity*            Informational (Level 4)

### **Configured for normal sequence numbering, received SABME** **182**

The Port record is configured for a maximum frame sequence number (Outstanding Frames) of seven or fewer, but a command was received setting the mode to allow up to 127.

*Severity*            Informational (Level 4)

### **Received FRMR, WXYZ="n", control field="n", V(s)="n", V(r)="n", CMD/RSP="n"** **197**

The RLP HDLC frame processor task received a frame reject (FRMR) response to a previously transmitted frame.

*Severity*            Major (Level 2)

*Action*             The system recovers automatically from this error; however, if the message is repeated, it may mean that you have a bad communications line.

<b>SABM/DISC with wrong link address</b>	<b>198</b>
The HDLC frame processor task for the port has received an improperly addressed frame from the subscriber. This situation usually occurs when the port and subscriber devices are both configured as logical DCEs or logical DTEs.	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	Modify the Port record so that one end of the connection is a logical DCE and the other is a logical DTE.
<b>Illegal TC/Gen Clk Combination</b>	<b>219</b>
The software has determined that a port is set to run at an illegal line speed (throughput class).	
<i>Severity</i>	Critical (Level 1)
<i>Action</i>	This is probably a configuration error. Check the Port record and change the throughput class, if necessary.
<b>Excessively noisy line</b>	<b>250</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the communications line and cables.
<b>LP Buf Usage exceeded T: "n" C: "n"</b>	<b>304</b>
The RLP statistic <b>Percentage of Buffers in Use</b> has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	If this happens frequently, you may need to reroute some traffic.
<b>LP Msg Queued exceeded T: "n" C: "n"</b>	<b>305</b>
The RLP statistic <b>Number of Queued Messages</b> has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	If this happens frequently, you may need to reroute some traffic.
<b>LP Rcv Frm/Sec exceeded T: "n" C: "n"</b>	<b>306</b>
The RLP statistic <b>Received Frames/Sec</b> has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	If this happens frequently, you may need to reroute some traffic.

**LP Trn Frm/Sec exceeded T: "n" C: "n" 307**

The RLP statistic **Transmitted Frames/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, you may need to reroute some traffic.

**LP Rej Frm/Sec exceeded T: "n" C: "n" 308**

The RLP statistic **Rejected Frames/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise and check for configuration errors on both the FRX port and the connected user device.

**LP Rtrn Frm/S exceeded T: "n" C: "n" 309**

The RLP statistic **Retransmitted Frames/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise and check for configuration errors on both the FRX port and the connected user device.

**Rcv Frm/Sec exceeded T: "n" C: "n" 311**

The port statistic **Received Frames/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, you may need to reroute some traffic.

**Tran Frm/Sec exceeded T: "n" C: "n" 312**

The port statistic **Transmitted Frames/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, you may need to reroute some traffic.

**RTrn Frm/Sec exceeded T: "n" C: "n" 313**

The port statistic **Retran Frames/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise, and check for configuration errors on both the FRX port and the connected user device.



**FCS Rej/Sec exceeded T: "n" C: "n"****314**

The port statistic **FCS Errors/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.) A value consistently greater than zero indicates line problems.

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise, and check for configuration errors on both the FRX port and the connected user device.

**Log Rej/Sec exceeded T: "n" C: "n"****315**

The port statistic **Logical Rejects/Sec** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.) A value consistently greater than zero indicates line problems.

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise, and check for configuration errors on both the FRX port and the connected user device.

**Trn Err Ratio exceeded T: "n" C: "n"****316**

The port statistic **Transmit Error Ratio** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise, and check for configuration errors on both the FRX port and the connected user device.

**Rcv Err Ratio exceeded T: "n" C: "n"****317**

The port statistic **Receive Error Ratio** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, check the line for noise, and check for configuration errors on both the FRX port and the connected user device.

**Rcv Port Usage exceeded T: "n" C: "n"****318**

The port statistic **% Receive Port Utilization** has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)

*Severity* Informational (Level 4)

*Action* If this happens frequently, you may need to add ports or reroute some traffic.

<b>Trn Port Usage exceeded T: "n" C: "n"</b>		<b>319</b>
The port statistic % <b>Transmit Port Utilization</b> has exceeded the threshold (T: "n") that was set by the user. (C: "n" is the current value.)		
<i>Severity</i>	Informational (Level 4)	
<i>Action</i>	If this happens frequently, you may need to add ports or reroute some traffic.	
 <b>Receive Yellow Alarm Condition Set</b>		 <b>338</b>
A Yellow Alarm was received.		
<i>Severity</i>	Major (Level 2)	
<i>Action</i>	Contact your T1 carrier.	
 <b>Receive Yellow Alarm Condition Set</b>		 <b>339</b>
The condition that caused event 338 has been cleared		
<i>Severity</i>	Informational (Level 4)	
 <b>LIC "n" Installed, Not Configured</b>		 <b>377</b>
The specified Line Interface Card (LIC) exists in the node, but has not been configured in the Line Processor file.		
<i>Severity</i>	Minor (Level 3)	
<i>Action</i>	Configure the LIC or remove it from the node.	
 <b>LIC "n" Configured, Not Installed</b>		 <b>378</b>
The specified Line Interface Card (LIC) has been configured in the Line Processor file, but does not exist in the node.		
<i>Severity</i>	Critical (Level 1)	
<i>Action</i>	Install the LIC or delete its record.	
 <b>LIC "n" Config Mismatch—Type "n"</b>		 <b>379</b>
The interface type of the specified Line Interface Card (LIC) installed in the node is different from the interface type configured in the Line Processor file. As a result, the software does not load properly and will not operate.		
<i>Severity</i>	Major (Level 2)	
<i>Action</i>	Change either the card or the file.	
 <b>Link Enabled</b>		 <b>400</b>
The port has been enabled from the On-Line Port Operations menu.		
<i>Severity</i>	Major (Level 2)	

---

<b>Link Disabled</b>	<b>401</b>
The port has been disabled from the On-Line Port Operations menu.	
<i>Severity</i>	Major (Level 2)
<b>Link Disconnected</b>	<b>402</b>
For X.25, this means that the link is disconnected and level 2 cannot be established.	
For SNA TPAD, this means that an XID command frame has been issued by the TPAD, but either there has been no response or the received XID data does not match the XID data configured for the TPAD subscriber.	
For SNA HPAD, this means that no XID or SNRM command frame has been received for any link address configured for the HPAD subscriber.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the hardware at both ends to make sure the devices are operational and cables are securely connected. For SNA, also check the configuration records to make sure they match the HPAD/TPAD.
<b>Link Up</b>	<b>403</b>
The level 2 link is up.	
<i>Severity</i>	Major (Level 2)
<b>X.25 Link Failed</b>	<b>404</b>
The link has failed; some modem controls are not present, and the physical link is down.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the modem and cables for secure connections and proper operation.
<b>Restart with cc “n” dc “n”</b>	<b>405</b>
A Restart has been issued, with the cause code (cc) and diagnostic code (dc) shown.	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	Depends on the cause. If necessary, contact your service representative.

<b>Operational</b>	<b>406</b>
For all ports except those noted below, this means that the link is up.	
For SNA TPAD, this means that the XID exchange has been performed, and the XID data received in the response frame matches the XID data configured for the TPAD subscriber. The link is ready to establish an X.25 connection with the remote HPAD.	
For SNA HPAD, this means that an XID or SNRM command frame has been received for at least one of the link addresses configured for the HPAD subscriber. The link is ready to establish an X.25 connection with the remote TPAD.	
<i>Severity</i>	Major (Level 2)
<b>Call Ctr LCN = "n" cc = "n" dc = "n"</b>	<b>407</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	Depends on the cause. If necessary, contact your service representative.
<b>End of IPL</b>	<b>408</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>PVC is Up</b>	<b>409</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>PVC Reset</b>	<b>410</b>
A Reset was sent on the PVC.	
<i>Severity</i>	Informational (Level 4)
<b>Received Reset LCN = "n", cc = "n" dc = "n"</b>	<b>411</b>
A Reset was received on the designated LCN, with the cause code <b>cc</b> and diagnostic code <b>dc</b> .	
<i>Severity</i>	Informational (Level 4)
<b>Received Reset Confirm</b>	<b>412</b>
A Reset Confirmation was received.	
<i>Severity</i>	Informational (Level 4)

<b>PAD Link Failed</b>	<b>413</b>
Self-explanatory.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the async PAD port and its cables for proper operation and secure connection.
<b>Beginning of Congestion</b>	<b>414</b>
The level of Maximum Congestion specified in the Node Defaults record has been exceeded, and no more events will be put into the event buffer until the Minimum Congestion level (also specified in the Node Defaults record) has been reached.	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	If this occurs frequently, you may want to increase the level of Maximum Congestion specified in the Node Defaults record.
<b>End of Congestion, “n” events lost</b>	<b>415</b>
The Minimum Congestion level has been reached. (See event 414, above.)	
<i>Severity</i>	Informational (Level 4)
<b>PAD Autocall Retries Exhausted</b>	<b>416</b>
The async PAD retry timer has expired without a connection being established.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	None; however, if this occurs with any frequency, you may want to increase the timer ( <b>Retry Count</b> ) or check the remote async device for problems.
<b>Frame Relay Link Failed</b>	<b>417</b>
The physical link is down.	
<i>Severity</i>	Critical (Level 1)
<i>Action</i>	Check the cables for secure connections and proper operation.
<b>PU Status p = “n” stn = 0x”n” status = “n”</b>	<b>426</b>
The SDLC PU status has changed.	
<i>Severity</i>	Major (Level 2)

<b>Duplicate of DLCI “n” on Port</b>	<b>428</b>
Each connection sharing a DLCI must be on a different logical port, and two records have been configured in the FRX specifying the same logical port on one DLCI. (DLCIs are configured in records for logical ports, IP/LLC2/IPX interfaces over frame relay, and frame relay PVCs.) Only one of the duplicate connections will come up.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the database records for the duplicate configuration and change one (or more) of the records.
<b>File Update: FRDLCI.DAT</b>	<b>429</b>
The Frame Relay DLCI configuration file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Received Port Disable Request</b>	<b>430</b>
Self-explanatory.	
<i>Severity</i>	Critical (Level 1)
<i>Action</i>	None; however, all users of this port should be made aware of the disable.
<b>Received Port Dump Request</b>	<b>431</b>
The BSC device has experienced a problem that caused it to send a request to send a dump to the port.	
<i>Severity</i>	Critical (Level 1)
<i>Action</i>	Check the device.
<b>Node Under Remote Control</b>	<b>432</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Remote Control Released</b>	<b>433</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Remote Control CXN Clr cc= “n” dc = “n”</b>	<b>434</b>
A remote control connection was cleared.	
<i>Severity</i>	Informational (Level 4)
<i>Action</i>	Depends on the cause.

<b>LG Buffer MALLOC Problem PKTs Lost</b>	<b>435</b>
This applies to a debug tool used by service personnel, and will not appear under normal operation.	
<i>Severity</i>	Major (Level 2)
<b>RCV Unknown Event Code from Net.</b>	<b>436</b>
An unknown event was received from the network.	
<i>Severity</i>	Major (Level 2)
<b>RCV Invalid Event Format from Net.</b>	<b>437</b>
The node has received an event with an invalid format.	
<i>Severity</i>	Informational (Level 4)
<b>DOS Error Handler Exceeded Limit</b>	<b>438</b>
The FRX was performing a DOS operation and, for some reason, could not reach DOS.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Reboot the node and watch for error messages during boot-up. If the problem persists, contact your service representative.
<b>Database Error, Access Restricted</b>	<b>439</b>
The database is inconsistent with what the software expects.	
<i>Severity</i>	Critical (Level 1)
<i>Action</i>	Contact your service representative.
<b>Abrev Addr File Upd: ABVSUB.DAT</b>	<b>440</b>
The Abbreviated Address file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Async Init File Upd: ASYSETUP.DAT</b>	<b>441</b>
The Async Console file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>BSC Device File Upd: BSCDSP.DAT</b>	<b>442</b>
The BSC Interactive Devices file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>LP Config File Upd: LPTYPE.DAT</b>	<b>443</b>
The Line Processor configuration file has been updated.	
<i>Severity</i>	Informational (Level 4)

<b>Port Config File Upd: PRTPAR.DAT</b>	<b>445</b>
The Port configuration file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Pad Profile File Upd: PROFILE.DAT</b>	<b>446</b>
The Async PAD Profile file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>PVC Config File Upd: PVCSUB.DAT</b>	<b>447</b>
The PVC Subscriber file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Rmt Subscriber File Upd: RSNSVC.DAT</b>	<b>448</b>
The Remote Subscriber file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Subscriber File Upd: SVCSUB.DAT</b>	<b>449</b>
The SVC Subscriber file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Statistic Def File Upd: STDPAR.DAT</b>	<b>450</b>
The Default Statistics Parameters file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Translation File Upd: XLTPAR.DAT</b>	<b>451</b>
The X.25 Address Translation Template file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>X.25 Default File Upd: X25REC.DAT</b>	<b>452</b>
The Node file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Alarm Enable File Upd: ERRMSG.TXT</b>	<b>453</b>
The Alarms file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Remote Update File Upd: UPDATE.TXT</b>	<b>454</b>
A software update has been sent.	
<i>Severity</i>	Informational (Level 4)



---

<b>Login Password Changed</b>	<b>455</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Operator Logged into Node</b>	<b>456</b>
An async terminal operator has logged into the node via an async PAD port.	
<i>Severity</i>	Informational (Level 4)
<b>Operator Logged out of Node</b>	<b>457</b>
The async terminal operator has logged out of the node via the async PAD port.	
<i>Severity</i>	Informational (Level 4)
<b>PAD Login File Upd: PADLOG.DAT</b>	<b>458</b>
The Login file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>IP Route File Upd: IPRSUB.DAT</b>	<b>459</b>
The IP Routing file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>IP Interface File Upd: IPRSUB.DAT</b>	<b>460</b>
The IP Routing file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>X.25 CUG File Updated: CUGPAR.DAT</b>	<b>461</b>
The Closed User Group file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>SNMP Trap File Upd: TRPPAR.DAT</b>	<b>462</b>
The SNMP Trap Routing file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>SNMP Community File Upd: COMPAR.DAT</b>	<b>463</b>
The SNMP Community Table file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>LP Buf Usage Under Threshold</b>	<b>464</b>
The situation that caused event 304 has ended.	
<i>Severity</i>	Informational (Level 4)

<b>LP Msg Queued Under Threshold</b>	<b>465</b>
The situation that caused event 305 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>LP Rcv Frm/Sec Under Threshold</b>	<b>466</b>
The situation that caused event 306 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>LP Trn Frm/Sec Under Threshold</b>	<b>467</b>
The situation that caused event 307 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>LP Rej Frm/Sec Under Threshold</b>	<b>468</b>
The situation that caused event 308 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>LP Rtrn Frm/S Under Threshold</b>	<b>469</b>
The situation that caused event 309 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>Rcv Frm/Sec Under Threshold</b>	<b>471</b>
The situation that caused event 311 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>Tran Frm/Sec Under Threshold</b>	<b>472</b>
The situation that caused event 312 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>ReTran Frm/Sec Under Threshold</b>	<b>473</b>
The situation that caused event 313 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>FCS Rej/Sec Under Threshold</b>	<b>474</b>
The situation that caused event 314 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>Log Rej/Sec Under Threshold</b>	<b>475</b>
The situation that caused event 315 has ended.	
<i>Severity</i>	Informational (Level 4)
<b>Tran Err Ratio Under Threshold</b>	<b>476</b>
The situation that caused event 316 has ended.	

<i>Severity</i>	Informational (Level 4)	
<b>Rcv Err Ratio Under Threshold</b>		<b>477</b>
	The situation that caused event 317 has ended.	
<i>Severity</i>	Informational (Level 4)	
<b>Port Rcv Usage Under Threshold</b>		<b>478</b>
	The situation that caused event 318 has ended.	
<i>Severity</i>	Informational (Level 4)	
<b>Port Trn Usage Under Threshold</b>		<b>479</b>
	The situation that caused event 319 has ended.	
<i>Severity</i>	Informational (Level 4)	
<b>Delete failed—nonexistent interface “n”</b>		<b>480</b>
	An IP Interface database record was created for a nonexistent interface. Someone then deleted the record (using [F4]), which caused this message to be generated.	
<i>Severity</i>	Informational (Level 4)	
<b>No mem avail processing intface “n”</b>		<b>481</b>
	The FRX6000 RLP did not have enough available memory to add the specified interface.	
<i>Severity</i>	Minor (Level 3)	
<i>Action</i>	Contact Netlink Support.	
<b>Can’t add interface “n”—IPadr err</b>		<b>482</b>
	Self-explanatory.	
<i>Severity</i>	Minor (Level 3)	
<i>Action</i>	Double-check the configured addresses.	
<b>Error adding interface “n”</b>		<b>483</b>
	Self-explanatory.	
<i>Severity</i>	Minor (Level 3)	
<i>Action</i>	Contact Netlink Support.	
<b>Error modifying interface “n”</b>		<b>484</b>
	Self-explanatory.	
<i>Severity</i>	Minor (Level 3)	
<i>Action</i>	Double-check the database record.	

<b>Interface “n” deleted successfully</b>	<b>485</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Interface “n” added successfully</b>	<b>486</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Interface “n” modified successfully</b>	<b>487</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Error deleting route with destination “n,” mask “n,” router “n”</b>	<b>488</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Contact Cabletron Systems’ Global Call Center.
<b>Route with destination “n,” mask “n,” router “n” deleted successfully</b>	<b>489</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>Error adding route with destination “n,” mask “n,” router “n”</b>	<b>490</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Cabletron Systems’ Global Call Center.
<b>Route with destination “n,” mask “n,” router “n” added successfully</b>	<b>491</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>BAG “n” capped at “n” but trunk MAXDPS “n”</b>	<b>492</b>
The data packet size (MAXDPS) on the trunk caused a greater traffic load than the configured Bandwidth Allocation Class (Group) would allow, so the software adjusted the bandwidth allocated to this trunk.	
<i>Severity</i>	Minor (Level 3)
<b>IPX Route File Upd: IPXRSUB.DAT</b>	<b>493</b>
The IPX Route file has been updated.	
<i>Severity</i>	Informational (Level 4)

<b>Alloc Error on Master SNMP Agent</b>	<b>494</b>
A buffer could not be allocated to process an SNMP message.	
<i>Severity</i>	Critical (Level 1)
<b>BPAD: Invalid Q Pkt “n”—PL</b>	<b>500</b>
An invalid Q packet has been received, disabling the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Configure the LIC or remove it from the node.
<b>BPAD: Invalid Pkt “n”—PL</b>	<b>501</b>
An invalid packet has been received, disabling the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BPAD: Invalid MSG “n”—Link</b>	<b>502</b>
An invalid message has been received, disabling the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BPAD: Invalid MSG “n”—Exchange</b>	<b>503</b>
An invalid message has been received, disabling the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BPAD: Invalid CUA “n” DUA “n”</b>	<b>504</b>
An invalid message has been received, disabling the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>LINK: Invalid MSG fc “n”—BPAD</b>	<b>505</b>
An invalid message has been received, disabling the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid control block</b>	<b>513</b>
An error has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.

<b>BSCI: Invalid parameters</b>	<b>514</b>
One or more parameters specified in the Port Parameters record for this port is invalid. This error disables the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Correct the Port Parameters record, then reenable the port ( <b>[B]</b> , <b>[A]</b> , <b>[C]</b> from the Main Menu). If this doesn't work, take the same action as for message 500.
<b>BSCI: Invalid port number or type</b>	<b>515</b>
The port number and/or type specified in the Port record is not valid for BSC Interactive.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the Port record.
<b>BSCI: Invalid message transfer</b>	<b>516</b>
Self-explanatory. This error disables the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid circuit operations</b>	<b>517</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid state event action</b>	<b>518</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid buffer operations</b>	<b>519</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid CRC operations</b>	<b>520</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.

<b>BSCI: Invalid queue operations</b>	<b>521</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid protocol operations</b>	<b>522</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>BSCI: Invalid CUA, DUA operations</b>	<b>523</b>
An invalid operation has occurred and has disabled the port.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Take the same action as for message 500.
<b>Invalid Line Speed LP “n” Port “n”</b>	<b>524</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Correct the line speed in the Port record.
<b>I-FRM Blocked-Remote Busy Timeout</b>	<b>530</b>
An RNR (Receive Not Ready) condition on the port has been cleared by expiration of the Remote Busy Timer, which caused the port to be reset.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the user device for a problem that caused the RNR.
<b>I-FRM Blocked-No Acks from Remote</b>	<b>531</b>
The remote user device is not accepting transmission from the local device, and the local port has been reset.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the remote device for a problem.
<b>Enter Service Affecting Condition</b>	<b>532</b>
The DTE and DCE exchange messages regularly so that each knows the other is running and ready. If one end does not respond, this event message is sent and the link goes down.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the equipment to see what caused the failure to respond.

<b>Exit Service Affecting Condition</b>	<b>533</b>
The situation that caused event 362 has ended.	
<i>Severity</i>	Major (Level 2)
<b>DLCI “n” Frm Relay PVC Disconnected</b>	<b>534</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>DLCI “n” Received Bad Frame</b>	<b>535</b>
Either the DLCI was not configured or the frame was on an unavailable DLCI.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Configure the DLCI or resent the frame.
<b>DLCI “n” No Response to STATUS ENQ</b>	<b>536</b>
There was no response to a status enquiry from the DTE.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the status of the DCE.
<b>DLCI “n” Flow Control On</b>	<b>537</b>
Flow control has been implemented on a frame relay port and data is queued.	
<i>Severity</i>	Minor (Level 3)
<b>DLCI “n” Frame Discarded—Flow Ctl</b>	<b>538</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	The frame must be resent.
<b>DLCI “n” Line does not exist</b>	<b>539</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the configuration records for the node, LP and port.
<b>DLCI “n” Not Configured</b>	<b>540</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Configure the DLCI in the port’s database record.



<b>DLCI “n” Frame Relay Header Invalid</b>	<b>541</b>
The header contained an invalid DLCI.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the configuration record for the port.
<b>DLCI “n” PVC does not exist</b>	<b>542</b>
Self-explanatory.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Create a PVC record.
<b>DLCI “n” Frame Discarded—CIR</b>	<b>543</b>
A frame was discarded, probably because the excess burst size (B <sub>E</sub> ) was exceeded.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	The frame must be resent.
<b>DLCI “n” frame relay PVC deleted</b>	<b>545</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>DLCI “n” frame relay PVC connected</b>	<b>546</b>
Self-explanatory.	
<i>Severity</i>	Informational (Level 4)
<b>DLCI “n” Data Received on Inactive PVC</b>	<b>547</b>
One end of the PVC is probably not up.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check both ends of the PVC.
<b>DLCI “n” No STATUS ENQ Received</b>	<b>548</b>
No Status Enquiry was received when one was expected.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Check the remote device.
<b>LLC Interface File Upd: LLC2IPAR.DAT</b>	<b>561</b>
The LLC2 Interface file has been updated.	
<i>Severity</i>	Informational (Level 4)

<b>LLC Host File Upd: LLC2HPAR.DAT</b>	<b>562</b>
The LLC2 Host file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>LLC LAN Card File Upd: LANPAR.DAT</b>	<b>563</b>
The LLC2 LAN Card file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>IPX Filter Def File Upd: IPXFPAR.DAT</b>	<b>564</b>
The IPX Filter Definitions file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>IPX Filt App File Upd: IPXFLTAP.DAT</b>	<b>565</b>
The IPX Filter Applications file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Bridge Filt Def File Upd: BRGFLTD.DAT</b>	<b>640</b>
The Bridge Filter Definitions file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Bridge Filt App File Upd: BRGFLTAP.DAT</b>	<b>641</b>
The Bridge Filter Applications file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>IPX Interface File Upd: IPXISUB.DAT</b>	<b>642</b>
The IPX Interfaces file has been updated.	
<i>Severity</i>	Informational (Level 4)
<b>Lan Card Number/Type Mismatch</b>	<b>643</b>
A mismatch has occurred between the LAN card type and the requested interface type when configuring a LAN-based IP or IPX interface.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Change the requested LAN card number or LAN card type.
<b>Fr RLP/PORT/DLCI Mismatch</b>	<b>644</b>
A mismatch has occurred between the current configuration and the requested RLP/Port/DLCI when configuring a frame relay based IP or IPX interface.	
<i>Severity</i>	Minor (Level 3)
<i>Action</i>	Change the requested RLP/Port/DLCI.

**Receive Loss of Sync condition Set** **650**

The receiving end of the connection has reported a loss of synchronization.

*Severity* Major (Level 2)

*Action* Check the T1/E1 cable at the local end of the connection. If it is securely connected and everything else appears operational, contact your carrier.

**Receive Carrier Loss condition Set** **651**

The receiving end of the connection has reported that the signal from the carrier is lost.

*Severity* Major (Level 2)

*Action* Check the T1/E1 cable at the local end of the connection. If it is securely connected and everything else appears operational, contact your carrier.

**Receive Remote Alarm condition Set** **652**

The remote device is not receiving the signal from the local device.

*Severity* Major (Level 2)

*Action* Check the T1/E1 cable at the local end of the connection. If it is securely connected and everything else appears operational, contact your carrier.

**Receive Loss of Sync condition Cleared** **653**

The situation that caused event 650 has been fixed. However, the T1/E1 connection will not be operational if any of events 650-652 have been set but not cleared.

*Severity* Informational (Level 4)

**Receive Carrier Loss condition Cleared** **654**

The situation that caused event 651 has been fixed. However, the T1/E1 connection will not be operational if any of events 650-652 have been set but not cleared.

*Severity* Informational (Level 4)

**Receive Remote Alarm condition Cleared** **655**

The situation that caused event 652 has been fixed. However, the T1/E1 connection will not be operational if any of events 650-652 have been set but not cleared.

*Severity* Informational (Level 4)

<b>SDLC Rem. Link Stn Not Responding</b>	<b>701</b>
Self-explanatory. ( <b>Rem Link Stn</b> is the Remote Link Station.)	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the PU to make sure it is operational.
<b>SDLC Link Stn Sent DM</b>	<b>702</b>
The link station sent a Disconnect Mode response, and the logical link is down.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Link Stn rcvd FRMR, Inv. cmd</b>	<b>704</b>
The remote device received an invalid command and responded with a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Stn rcvd FRMR, IFLD invalid</b>	<b>705</b>
The remote device received an unpermitted I frame and responded with a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Stn rcvd FRMR, Nr invalid</b>	<b>706</b>
The remote device received a frame with an invalid $N_{(r)}$ and responded with a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Stn rcvd FRMR, Ifld too long</b>	<b>707</b>
The remote device received an I frame that was too long and responded with a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Rem Stn sent Invalid Command</b>	<b>708</b>
The remote device received an invalid or unsupported command.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Rem Stn sent unexpected IFLD</b>	<b>709</b>
The remote device send an unpermitted I frame.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Rem Stn sent invalid Nr</b>	<b>710</b>
The remote device sent a frame with an invalid $N_{(r)}$ .	
<i>Severity</i>	Major (Level 2)

---

<b>SDLC Rem Stn Exceeded window size</b>	<b>711</b>
The number of frames sent by the remote device has exceeded the window size.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Station Inactivity time exp</b>	<b>712</b>
The timer defined by the parameters <b>No Response Poll Period</b> and <b>Maximum Retransmissions</b> in the SNA Port record has expired.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the PU to make sure it is operational.
<b>SDLC XID Retries exhausted</b>	<b>713</b>
The retry limit for XID has been exceeded and link establishment has failed.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Rem Stn sent FRMR—no reason</b>	<b>714</b>
The remote station sent a Frame Reject with no reason.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Remote RNR limit exceeded</b>	<b>715</b>
The remote station is busy. This could be a hardware or buffer problem in the remote device.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the hardware and configuration at the remote device.
<b>SDLC Rem Tx Frame exceeds MAXDATA</b>	<b>717</b>
A frame transmitted by the remote station exceeds the configured value for <b>Maximum Bytes per Frame</b> .	
<i>Severity</i>	Major (Level 2)
<b>SDLC Rem sent UA in NRM</b>	<b>718</b>
The remote station sent a UA while in Normal Response Mode, which is not allowed.	
<i>Severity</i>	Major (Level 2)
<b>SDLC No DSR on link</b>	<b>720</b>
A necessary DSR was not received from the DCE.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the modem to make sure it is operational.

<b>SDLC No CTS on link</b>	<b>721</b>
A necessary CTS was not received from the DCE.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the modem to make sure it is operational.
<b>SDLC No External Clock</b>	<b>722</b>
The necessary clock is not being provided.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the modem to make sure it is operational.
<b>SDLC LLC/2 Remote Link Stn lost</b>	<b>736</b>
The remote station is not responding. Either the Inactivity Timer ( <b>Ti</b> ) or Acknowledgment Timer ( <b>T2</b> ) has expired.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	Check the remote station to make sure it is operational.
<b>LLC/2 DM Received</b>	<b>737</b>
The remote station sent a Disconnect Mode response and the logical link is down.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 SABME Received when open</b>	<b>738</b>
The remote station sent a SABME to the local station, but the local station had already been initialized via a SABME—UA exchange.	
<i>Severity</i>	Major (Level 2)
<i>Action</i>	None; however, if the problem persists, contact your support representative.
<b>LLC/2 FRMR Rcvd, Invalid Command</b>	<b>739</b>
The remote device received an invalid or unsupported command, and returned a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Rcvd, IFLD not permitted</b>	<b>740</b>
The remote device received an I-frame when it was not permitted, and returned a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Rcvd, Invalid Nr</b>	<b>741</b>
The remote device received an invalid $N_{(R)}$ , and returned a Frame Reject.	
<i>Severity</i>	Major (Level 2)

<b>LLC/2 FRMR Rcvd, IFLD too long</b>	<b>742</b>
The remote device received an I frame that was too long, and returned a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Rcvd, Invalid Command</b>	<b>743</b>
The remote device received an invalid command or response, and returned a Frame Reject.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Sent, IFLD not permitted</b>	<b>744</b>
The remote device sent an I frame when it was not permitted, and a Frame Reject was returned.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Sent, Invalid Nr</b>	<b>745</b>
The remote device sent an invalid $N_{(R)}$ , and a Frame Reject was returned.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Sent, IFLD too long</b>	<b>746</b>
The remote device sent an I frame that was too long, and a Frame Reject was returned.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Sent, no reason</b>	<b>747</b>
Self-explanatory.	
<i>Severity</i>	Major (Level 2)
<b>LLC/2 FRMR Rcvd, no reason</b>	<b>748</b>
Self-explanatory.	
<i>Severity</i>	Major (Level 2)
<b>Excessive Link CRC errors</b>	<b>759</b>
Self-explanatory. The line will be shut down and reestablishment will be retried once every minute.	
<i>Severity</i>	Major (Level 2)
<b>SDLC Transmit link error</b>	<b>761</b>
Self-explanatory. The line will be shut down and reestablishment will be retried later.	
<i>Severity</i>	Major (Level 2)

**SDLC Link Stn rcv FRMR, Unexp. IFLD**

**762**

The remote station received an S or U frame with an unexpected I frame attached.

*Severity*            Major (Level 2)



# Configuring the Subscriber Table

*About the Subscriber Table and Subscriber IDs; accessing the Subscriber Table window; adding or modifying a subscriber table entry; editing the Routing and Address tables*

---

The Subscriber Table allows you to add or modify the entries your FRX or SmartSwitch 1800 will use to establish virtual connections to end-user devices in the network. These entries contain the assigned subscriber addresses, as well as information that links those addresses to a specific FRX or SmartSwitch 1800 physical or logical port (or ports). Entries also contain additional information related to preferred delivery algorithms, alternate routing paths, and transmission priority.



*The Subscriber Table applies to all serial ports, regardless of protocol; however, it is only available on devices running firmware version 3.3.0 or later.*

## About Subscriber IDs

Your FRX and SmartSwitch 1800 devices are designed to provide point-to-point dedicated connections among the devices communicating through their serial ports. There are two types of connections used to accomplish this: Permanent Virtual Circuits, or PVCs, which define permanent point-to-point connections which are always available, even when they are not being used; and Switched Virtual Circuits, or SVCs, which are established and broken in response to specific call requests.

Subscriber IDs are used to establish virtual connections between the FRX and end-user devices (or subscribers) in the network. A Subscriber ID is associated with at least one physical or logical port on your FRX or SmartSwitch 1800 device, and includes a number of parameters related to how call requests are routed to that subscriber. The Subscriber Table allows you to configure this subscriber information.

## Accessing the Subscriber Table

To launch the Subscriber Table:

1. In the Hub View, click on the **Device** button to display the Device menu.
2. Drag down to **Subscriber Table**, and release. The Subscriber Table window, [Figure 4-1](#), will appear.

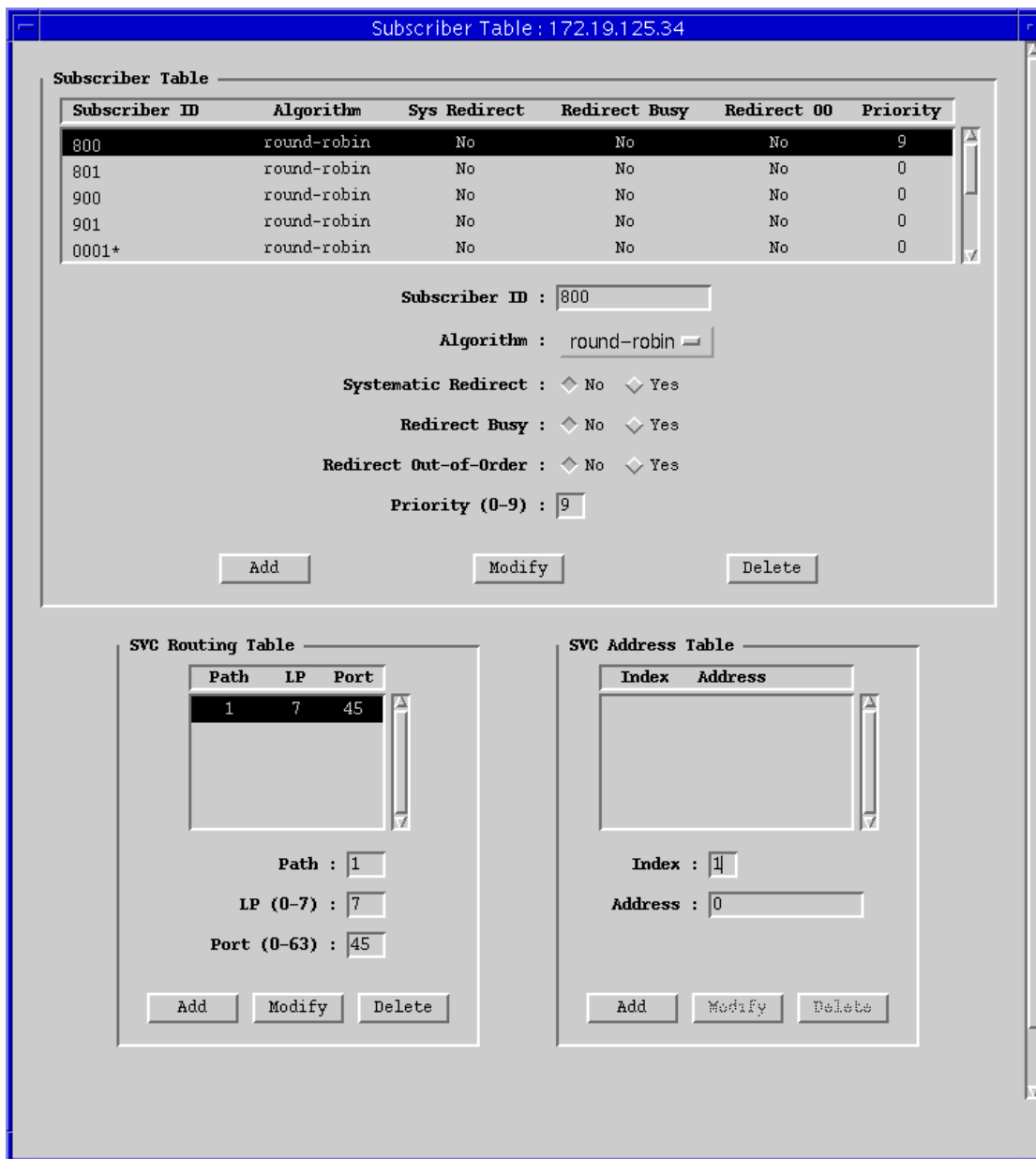


Figure 4-1. The Subscriber Table Window

The Subscriber Table window contains three main areas: the **Subscriber Table** itself (in the top half of the window), which allows you to add, modify, or delete subscriber entries; the **Routing Table** (on the lower left), which allows you to assign one or more routing paths to a subscriber entry by associating that entry with one or more physical or logical ports on your device; and the **Address Table** (on the lower right), which allows you to assign the addresses that will be used for call redirection (if those options are specified in the table entry). Each of these tables is described below.



*If no **Close** button appears in your window, use the scroll bar to the right of the display to access the button, which is at the bottom of the window.*

## Configuring the Subscriber Table

The Subscriber Table displayed at the top of the window is the main table that allows you to define the subscribers who will be communicating across your FRX or SmartSwitch 1800 device. To configure a Subscriber Table entry, you must set the following parameters:

### Subscriber ID

Each subscriber is identified by an ID, or address, of up to 15 digits. When assigning or editing a Subscriber ID, keep the following in mind:

- Subscribers using a public data network (PDN) must conform to the format used by the PDN. (A PDN is a network operated by common carriers or telecommunications administrations for the purpose of providing data transmission capabilities to the public.) For example, CCITT recommendation X.121 specifies a format which includes a one-digit international code, followed by a four-digit Data Network Identification Code (DNIC), followed by up to 10 digits of Network Terminal Number (NTN).
- A private network — one that will not communicate with other networks — can create its own format, using any or all of the available digits as desired.

Since each FRX or SmartSwitch 1800 port can support multiple subscribers, Subscriber IDs can also use wildcard characters so that all subscribers on a port can be referenced with a single entry. Two wildcard characters are available:

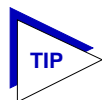
- A question mark (?) in a subscriber ID matches any single digit. For example, 3110???????? matches any 14-digit address that begins with 3110.
- An asterisk, or star (\*), matches any combination of digits, including none at all. For example, 3110\*00 is any address that starts with 3110 and ends with 00, including 311000 but excluding 31100 (overlapping is not allowed). An asterisk by itself matches any address.

Wildcard characters can also be combined: the address 3110??\* matches any address that begins with 3110 and contains at least two more digits.

### Algorithm

The algorithm field allows you to select the means by which call requests are forwarded to one of several routing paths assigned to the named subscriber. You can select from among four options:

Round Robin	As its name implies, this algorithm selects ports cyclically in numeric order (as configured in the Routing Table). If a selected port is unreachable or congested, call requests are forwarded on to the next port in sequence.
Line Failed	The Alternate Route on Line Failure algorithm selects the first listed port that is not in a failed state. If the selected port does not make the connection, the call request will be cleared, even if other ports are available.
Line Busy	The Alternate Route on Line Busy algorithm selects the first port that is not busy. If that port has failed, the next available port will be selected.
Least LCN	The Least LCN with Throughput algorithm selects the line with the smallest load, calculated using the weight (speed) and number of virtual circuits in use on that line. (Weights are assigned to each line in proportion to their throughput within the routing path.)



*The alternate routes used by these algorithms are specified in the Routing Table, described beginning on [page 4-5](#); if you do not wish to use a routing algorithm, simply accept the default setting and enter only one routing path.*

### Systematic Redirect

The Systematic Redirect field allows you to specify whether or not calls to the named subscriber will be automatically redirected to the first alternate subscriber specified in the Address Table (described beginning on [page 4-6](#)). If you select yes, the original subscriber is skipped and *all calls* designated for that subscriber will be redirected to the first alternate address, regardless of the condition of either path. Any additional configured alternate addresses are ignored.

### Redirect Busy

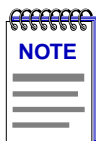
If you enable the Redirect Busy option, calls to the named subscriber will be redirected to the alternates listed in the Address Table if the primary subscriber device is busy. Again, be sure you've configured the alternate addresses in the Address Table.

### Redirect Out-of-Order

The Redirect on Out-of-Order option allows you to specify that calls to the named subscriber device will be redirected to the alternate subscribers if the primary device is out of order.

**Priority**

The Connection Priority field allows you to configure priorities for traffic within the device: the higher the number assigned to the subscriber, the higher the priority that subscriber's calls will receive relative to other intra-nodal traffic. These priorities have no effect on traffic exiting the device.



*Traffic priorities can also be configured for SNA ports with LLC2 connections, logical ports, LLC2 hosts, LLC2 interfaces, IP interfaces, IPX interfaces, and PVC connections. When configuring priorities, be sure to consider the types of traffic being routed on other connections in the node.*

## Configuring Routing Table Entries

So that virtual connections can be established with and by each of the subscribers defined in the Subscriber Table, you must associate each Subscriber ID with one or more physical or logical ports on your FRX or SmartSwitch 1800 device so that the call requests can be properly routed and the connection established. This is the function of the Routing Table. Entries which appear in this table are associated with the Subscriber ID currently selected in the Subscriber Table portion of the window; each Subscriber ID must have at least one routing table entry, or it will not function. If you configure more than one routing path (you're allowed up to eight), paths will be selected according to the algorithm specified in the Subscriber Table (see [page 4-4](#) for more information on routing algorithms).

Configuring a Routing Table entry requires the following information:

**Path**

Designates an index number assigned to the routing table entry; in some cases (depending on the algorithm specified for the selected subscriber table entry), this index value will define the order in which routing paths are selected when a call request is received. You can designate up to eight alternate routes for each subscriber entry; path values must be assigned sequentially.

**LP**

Designates the index number assigned to the RLP card which contains the physical or logical port you wish to assign to the selected Subscriber ID.

**Port**

Designates the index number assigned to the physical or logical port you wish to assign to the selected Subscriber ID. Indices 0-7 indicate physical ports; indices 8-63 indicate logical ports.

## Configuring Address Table Entries

If you have selected any redirect parameters for a Subscriber Table entry, you must use the Address Table to designate the alternate subscriber addresses that will be used by the redirect option(s) you have selected (see [page 4-4](#) for more information on redirect options). You can designate up to five alternate addresses for each subscriber table entry.

Each address table entry requires the following values:

### Index

The index value assigned to the address table entry. Some redirect options use this value to determine the order in which alternate addresses are selected. Allowable values are 1 - 5; values need not be assigned sequentially.

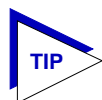
### Address

Use the address field to enter the Subscriber ID for any alternate subscribers you wish to associate with the selected subscriber table entry. These alternate addresses will be used by any enabled redirect options to determine alternate paths for call requests directed to the selected subscriber. Note that you cannot use wildcard characters in this field.

## Adding or Modifying Subscriber Table Entries

To add or modify a subscriber table entry:

1. If you wish to modify an existing entry, be sure that entry is highlighted in the Subscriber Table portion of the window.



*Remember, any additions or deletions to the Routing Table or the Address Table actually **modify** the selected Subscriber Table entry.*

2. In the **Subscriber Table** portion of the window:
  - a. Enter the appropriate **Subscriber ID** value. You can use up to 15 digits, including the question mark (?) and asterisk (\*) wildcards. For subscribers using a Public Data Network (PDN), be sure the ID you assign follows the code specifications for that network.
  - b. In the **Algorithm** field, select the means by which any alternate routing paths assigned to this subscriber will be selected. (Alternate routing paths are assigned via the Routing Table, as described in step 3.) If you do not wish to employ one of the available algorithms, simply accept the default value and assign only a single routing path.

- c. Click **Yes** on the **Systematic Redirect** option if you wish all calls to this subscriber to be redirected to the first alternate address defined in the Address Table. If you select this option, *no calls* will be received by the original subscriber, and only the first alternate subscriber will be used. Select **No** if you do not wish to redirect calls in this way.
  - d. Click **Yes** on the **Redirect Busy** option if you wish calls to this subscriber to be redirected to the defined alternate addresses when the original subscriber device is busy. Select **No** if you do not wish to redirect calls in this way.
  - e. Click **Yes** on the **Redirect Out-of-Order** option if you wish calls to this subscriber to be redirected to the defined alternate addresses when the original subscriber device is down. Select **No** if you do not wish to redirect calls in this way.
  - f. Use the **Priority** field to configure the priority level that will be assigned to this subscriber's calls relative to other intra-nodal traffic. The higher the priority value, the higher the priority assigned to that subscriber's calls. (Note that this value does not effect traffic exiting the device.)
  - g. Click on  to create a new entry, or on  to edit the entry currently selected in the Subscriber Table list box.
3. In the **Routing Table**:
- a. If you wish to modify an existing Routing Table entry, be sure that entry is selected (and remember, any changes you make to the Routing Table effect the Subscriber Table entry currently highlighted in the top portion of the window).
  - b. In the **Path** field, enter the index number you wish to assign to the path you are configuring. These index values will be used in some cases to determine the order in which the routing paths will be selected; note that these values must be assigned sequentially.
  - c. In the **LP** field, enter the index number of the RLP card which contains the physical or logical port you wish to use to reach the subscriber device. Note that, for an FRX4000 and SmartSwitch 1800, this value will always be zero.
  - d. In the **Port** field, enter the index number of the physical or logical port you wish to use to reach the subscriber device. Index values 0-7 refer to physical ports on the selected RLP; values 8-63 denote logical ports.
  - e. Click on  to create a new entry, or on  to edit the entry selected in the Routing Table list box. (Note that either adding or modifying a Routing Table entry automatically modifies the Subscriber Table entry highlighted in the Subscriber Table list box.)

4. In the **Address Table**:
  - a. If you wish to modify an existing Address Table entry, be sure that entry is selected (and remember, any changes you make to the Address Table effect the Subscriber Table entry currently highlighted in the top portion of the window).
  - b. In the **Index** field, enter the index value you wish to assign to the entry you are configuring. Allowable values are 1-5; these values need *not* be assigned sequentially.
  - c. In the **Address** field, enter the Subscriber ID assigned to the subscriber device you wish to use as a redirect option for the selected subscriber. How these addresses are used is dependent upon the redirect options selected for the Subscriber Table entry you're modifying. Note that you cannot use wildcards in this field.
  - d. Click on  to create a new entry, or on  to edit the entry selected in the Address Table list box. (Note that either adding or modifying an Address Table entry automatically modifies the Subscriber Table entry highlighted in the Subscriber Table list box.)
5. Click on  to exit the window.

## Deleting Table Entries

You can delete individual entries from any of the three tables in the window; keep in mind, however, that deleting a Routing Table or Address Table entry simply modifies the selected Subscriber Table entry; deleting a Subscriber Table entry also deletes all associated Routing Table and Address Table entries by default.

Remember, too, that deleting all Routing Table entries for a Subscriber Table entry invalidates the entry (as no path to the subscriber device is provided); deleting all Address Table entries for a Subscriber Table entry invalidates any enabled redirect options, since no redirect addresses will be defined.

To delete an entry from any of the tables:

1. Click to select the entry you wish to delete.
2. Click on . The selected entry will be removed. If you have deleted a Subscriber Table entry, all associated Routing Table and Address Table entries will also be removed.



# Frame Relay Status and Configuration

*About using the frame relay protocol; frame relay port and DLCI rate configuration; configuring frame relay backup groups; logical port configuration; viewing frame relay management, congestion, and error stats*

---

FRX and SmartSwitch 1800 ports which have been configured to use frame relay as their layer 2 protocol can be used to carry both frame relay traffic and traffic from other protocols which has been encapsulated in frame relay (per RFC 1490).

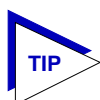
Each frame relay port can contain multiple logical ports — up to 56 on an FRX4000 and SmartSwitch 1800, and up to 56 per RLP on an FRX6000 — and each logical port is assigned a Data Link Connection Identifier (or DLCI), which identifies a point-to-point connection. All 56 logical ports can reside on one physical port, or be spread among several ports, and each can be configured to run one or more layer 3 protocols.

For each physical port configured to run frame relay, four configuration windows and three statistical windows are provided:

- The **Frame Relay Port Configuration** window allows you to configure basic operational parameters related to the frame relay protocol, and displays some general information about the serial port itself and the line to which it is connected;
- The **Frame Relay DLCI Rate Configuration** window allows you to select the data rate parameters for each DLCI configured on the selected frame relay port;
- The **Frame Relay Backup Groups** window allows you to configure backup groups for primary DLCI connections;
- The **Logical Port Configuration** window allows you to configure basic parameters related to logical port operation;

- **Frame Relay Management Stats** provide an overview of the frame management (LMI or Annex D) in use on the selected port, displayed via meters;
- **Frame Relay Congestion Stats** provide information about congestion notification and discard eligibility frames being transmitted across the port, also displayed in meters; and
- The **Frame Relay Errors** window provides a single meter, which displays the current frame discard rate.

These windows and their functions are described in the following sections.



*The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.*

## Configuring Frame Relay Ports

Two configuration windows allow you to set frame relay operational parameters for physical ports and specifications for any DLCI configured for a selected frame relay port: **Frame Relay Port Configuration**, described below, and **Frame Relay DLCI Rate Configuration**, described beginning on [page 5-8](#).

### Port Configuration

Using the Frame Relay Configuration window, you can configure some basic operational parameters for each of your frame relay ports.

To access the window:

1. Click mouse button 3 on the frame relay port of interest to display the Port Menu.
2. Drag down to **Frame Relay Port Configuration**, and release. The Frame Relay Configuration window, [Figure 5-1](#), will appear.

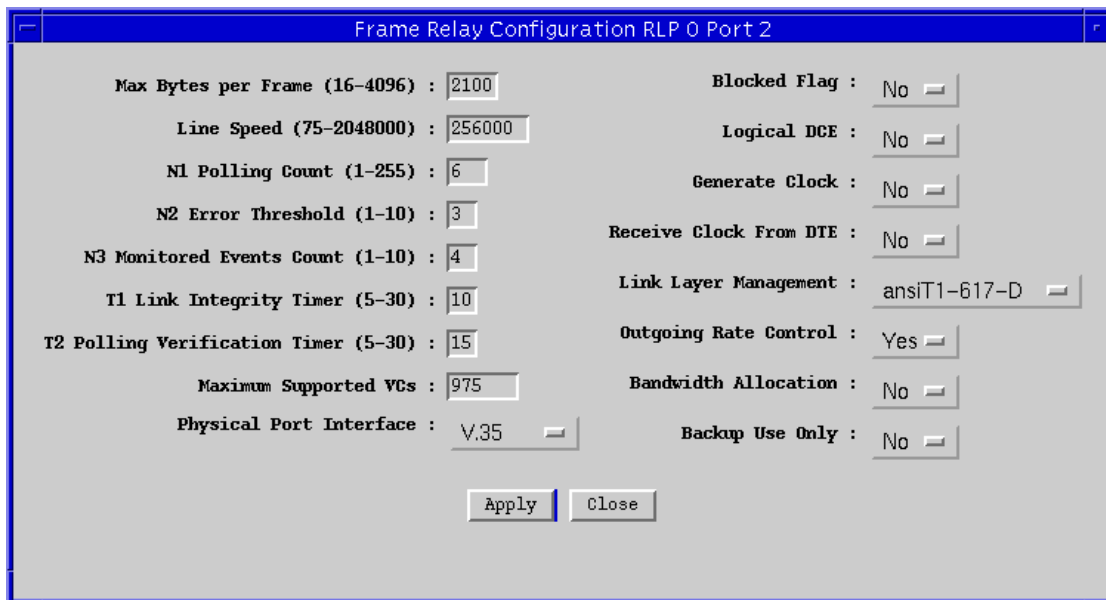


Figure 5-1. Frame Relay Port Configuration

The Frame Relay Configuration window provides the following information:

**Max Bytes per Frame**

This field specifies the size (in bytes) of the largest frame that can be transmitted across the port. This value is determined by your frame relay service provider.

**Line Speed**

This field specifies the data transmission rate in bits per second. If this port is a physical DTE, specify the line speed that matches the speed of the device connected directly to the port. If the port is a physical DCE (i.e., the attached I/O cable is DCE) specify the clock speed of the serial port you are configuring.

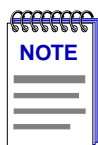
Possible line speed entries are:

75	64000	512000	1008000	1472000
150	72000	560000	1024000	1512000
300	112000	576000	1064000	1536000
600	128000	616000	1088000	1568000
1200	168000	640000	1120000	1600000
2400	192000	672000	1152000	1624000
4800	224000	704000	1176000	1664000
9600	256000	728000	1216000	1668000
14400	280000	768000	1232000	1728000
19200	320000	784000	1280000	1792000
24000	336000	832000	1288000	1856000
28800	384000	840000	1344000	1920000
38400	392000	896000	1400000	1984000
48000	448000	952000	1408000	2048000
56000	504000	960000	1456000	

If you enter a value that is within the valid range but not equal to one of the values listed above, the speed will be rounded up. If an RS-232 DCE port is directly connected to the DTE via the standard Cabletron cable, the maximum supported speed is 64000. If longer cabling is used, the maximum speed is 19200.

### N1 Polling Count

The Polling Count specifies the number of polling cycles that must pass between requests for full status reports, which include the status of all PVCs configured on the physical link. At an interval specified by the **T1 Link Integrity Timer** (described below), the logical data terminal equipment (DTE, or user-side equipment, typically a workstation or router) will send a status enquiry to its attached DCE (or network-side equipment), requesting the status of the network link. Each exchange of one enquiry and one response (or status message) defines one polling cycle. After the number of cycles specified by this value, a request for a full status report will be sent.



*If this port is configured as the logical data communications equipment (DCE), status enquiries will be initiated at its attached DTE (or user-side equipment), and the local node will respond with status messages. You can determine which link partner is the logical DTE and which is the logical DCE (network-side equipment) by checking the **Logical DCE** field in this window (described below).*

### N2 Error Threshold

The error threshold defines the number of link reliability and/or protocol errors that can occur during the period defined by the **N3 Monitored Events Count** (described below) before the logical DCE is declared inactive.

### N3 Monitored Events Count

The monitored events count defines the number of error-free polling cycles that must occur before the DCE is declared active if the first poll resulted in an error. If the first poll is error-free, the DCE is declared active immediately.

If the **N2 Error Threshold** is exceeded during the N3 count, the DCE will be declared inactive, and the N3 count will be restarted.

### T1 Link Integrity Timer

This value determines how often (in seconds) the logical DTE will initiate a status enquiry to its connected DCE, checking the status of the network link. Note that this value only has an effect when the selected port has been configured as the DTE (or user-side equipment); see **N1 Polling Count**, above, for more information.

### T2 Polling Verification Timer

The T2 Polling Verification Timer determines how long (in seconds) the logical DCE will wait for a status enquiry from its attached DTE before recording an error. This value only has an effect when the selected port has been configured as the DCE.

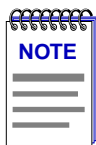
### Maximum Supported VCs

This value defines the maximum number of virtual circuits (or DLCIs) that can be supported by the selected serial port. This value is generally determined by your frame relay service provider.

### Physical Port Interface

The physical port interface is defined by the port's connector and cabling type, and must be configured as follows:

- For the FRX4000 and SmartSwitch 1800, port 0 and port 1 are always RS-232;



*If you have installed the optional CSU/DSU card on an FRX4000 or SmartSwitch 1800, it will logically take port 1, and you must configure certain CSU/DSU parameters through console management. Refer to your FRX or SmartSwitch 1800 hardware documentation for more information.*

- For the FRX4000, ports 2 and 3 are determined by the attached cables: RS-232, V.35, RS-449, or X.21;
- For the SmartSwitch 1800, ports 2 and 3 are determined by the attached cables: RS-232, V.35, or RS-449;
- For the FRX4000, ports 4-7 are determined by the expansion Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, and X.21. (RS-449 and X.21 interfaces require an RS-422 LIC.)

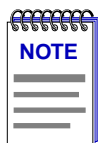
- For the FRX6000, ports 0-7 on each RLP are determined by the Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, RS-530 and X.21. (RS-449, RS-530, and X.21 interfaces require an RS-422 LIC.)

### Blocked Flag

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or re-booted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed.

### Logical DCE

This parameter defines the port's role as logical DCE (if **Yes**) or logical DTE (if **No**). The port configured as the DTE serves as the user-side equipment, sending data to an interface device (DCE, or network-side equipment) for encapsulation in a frame relay frame and transmission onto the frame relay network. The DTE also receives de-encapsulated data from the DCE for transmission onto its local network. Each port must be configured for the opposite value of that configured for its link partner — that is, a logical DCE must be connected to a logical DTE, and vice versa.



*Note that logical and physical DCE and DTE settings are independent of one another; a port can be both a **logical DTE** and a **physical DCE**.*

### Generate Clock

This setting specifies whether the port will generate the clock, or timing, necessary to synchronize traffic over the link. If the port is a physical DCE (as determined by the port's I/O cable interface), specify **Yes**, since the physical DCE generates clock. If the port is a physical DTE, specify **No**.

### Receive Clock from DTE

If this parameter is set to **Yes**, it allows the clock (timing) signal to be looped back from the DTE using the Terminal Timing (TT) signal, which can be helpful on high-speed lines. Generally, if the local interface is a physical DCE and the line speed is above 256 Kbps, this parameter should be set to **Yes**; however, make sure the DTE is configured to provide the terminal timing.

### Link Layer Management

When Link Layer Management is active, the protocol in use will verify and maintain the integrity of the link. The setting of this value determines whether link status enquiries will be used, and what form they will take:

no LMI	No Local Management Interface (LMI). No status enquiries will be used; this setting essentially disables frame relay's management abilities. LMI will prevent any
--------	---

links from becoming operational unless all DLCI rate settings match at both ends of the connection; without LMI, mismatched links may become operational, but they will behave unpredictably.

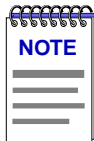
LMI rev 1	enquiries from the Local Management Interface (LMI) will be used;
ansiT1 617 D	enquiries in ANSI T1.617 Annex D format (an ANSI standard LMI) will be used.

### Outgoing Rate Control

This parameter determines whether the rate parameters (CIR, B<sub>C</sub>, and B<sub>E</sub>) assigned to the physical link and/or its virtual circuits will be enforced: **Yes** or **No**. Choosing not to enforce rate parameters allows traffic rates to exceed those configured for the selected circuits, possibly impacting performance. Exceeding CIR may also lead to additional charges from your frame relay provider.

### Bandwidth Allocation

If you have configured Bandwidth Allocation Groups for the selected port (or any logical ports configured for that port), you can use this field to enable (**Yes**) or disable (**No**) any configured bandwidth allocation parameters. BAGs regulate bandwidth usage by outgoing traffic on the physical link and can ensure that response time-sensitive traffic gets access to the available frame relay bandwidth. Up to 16 groups can be defined and configured through console management (refer to your FRX or SmartSwitch 1800 hardware documentation for more information).



*Bandwidth allocation groups cannot currently be configured via SPMA; for more information on configuring these groups, see your FRX or SmartSwitch 1800 hardware documentation.*

### Backup Use Only

This field determines whether all DLCIs on the port will be reserved exclusively as backups for other DLCIs in the same node. If you select **Yes**, this port will only provide backup DLCIs; if you select **No**, it can provide backup and primary DLCIs.

If you configure the port for backup use only, make sure no DLCIs on the port have been configured on an IP, IPX, or LLC2 interface. If this parameter is set to **Yes**, the port will remain disabled until needed for backup.

### Changing Configuration Values

You can edit the values in any field; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.

If you have made changes to the fields but would like to revert back to the previous values, click on the **Refresh** button.

3. Click on  to save your changes.

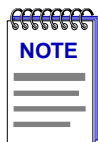
### Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

### DLCI Rate Configuration

The Frame Relay DLCI Rate Configuration window allows you to set traffic-related operational parameters for each DLCI configured for a selected frame relay port. Note that the values for these parameters will typically be set by your frame relay provider; they cannot be freely altered.



*When configuring DLCI rate values in this window, be sure to use the DLCI identifiers which apply to the logical ports configured for the serial port you've selected.*

To access the window:

1. Click mouse button 3 on the frame relay port of interest to display the Port menu.
2. Drag down to **Frame Relay DLCI Rate Configuration**, and release. The Frame Relay DLCI Table window, [Figure 5-2](#), will appear.



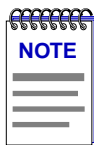
DLCI	CIR (In)	Bc (In)	Be (In)	CIR (Out)	Bc (Out)	Be (Out)	BECN	Priority	Bkup Grp	Bkup Protocol	State
18	128	128	0	64	64	0	1	0	10	Disabled	Active
20	64	64	0	32	32	0	0	0	0	Disabled	Active
70	256	256	0	60	60	0	0	0	0	Disabled	Active
85	128	128	0	72	72	0	0	0	0	Disabled	Active
86	128	128	0	64	64	0	0	0	0	Disabled	Active
500	128	128	0	64	64	0	0	0	0	Disabled	Active

DLCI : 18      Be (Out) : 0  
 CIR (In) : 128      BECN : 1  
 Bc (In) : 128      Priority : 0  
 Be (In) : 0      Backup Group : 10  
 CIR (Out) : 64      Backup Protocol : Disabled  
 Bc (Out) : 64      State : Active

Add    Modify    Delete  
 Refresh    Close

Figure 5-2. Frame Relay DLCI Table

The Frame Relay DLCI Table window allows you to configure the following parameters for each DLCI:



*In the DLCI Table you can configure Primary and Backup DLCIs. If you are configuring a primary DLCI, there are six additional parameters that can only be configured through console management. They are: Remote RLP, Remote Port, Remote DLCI, Switchover Timer, Switchback Timer, and Time to Hold Data While Waiting. For information on configuring these parameters, refer to your FRX or SmartSwitch 1800 hardware documentation.*

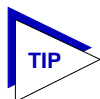
**DLCI**

Use this field to enter the identifier (16 - 991) for the DLCI whose traffic parameters you wish to configure. These DLCI numbers are typically assigned by your frame relay service provider.

**CIR (In/Out)**

Use this field to enter the Committed Information Rate (CIR) assigned to the selected DLCI by your frame relay provider. This value defines the amount of data guaranteed to be transmitted over the carrier’s network. Any burst of data

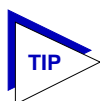
above the defined CIR can be marked as discard eligible (DE); frames with the DE bit set are considered to be excess data, and will be discarded if the network becomes congested.



*If congestion occurs on the selected DLCI while throughput is greater than the CIR, and the **Outgoing Rate Control** parameter (settable via the Frame Relay Port Configuration window, described beginning on [page 5-2](#)) is set to **Yes**, the throughput will immediately drop to the CIR level.*

### **B<sub>C</sub> (In/Out)**

Use this field to enter the Committed Burst Size (B<sub>C</sub>) assigned to the selected DLCI by your frame relay provider. The committed burst size defines the maximum amount of data (in bits) that the network agrees to transfer, under normal conditions, during a time interval T<sub>C</sub>. T<sub>C</sub> (also called the “bandwidth interval”) is calculated by dividing the committed burst size (B<sub>C</sub>) by the committed information rate (CIR); it defines the time interval during which the user can send only B<sub>C</sub> amount of data and B<sub>E</sub> excess data (see definition of B<sub>E</sub>, below). Any traffic which exceeds this burst rate will be marked discard eligible (DE), and discarded if the network becomes too congested. While sustained B<sub>C</sub> traffic rates are not guaranteed, B<sub>C</sub> traffic has a higher delivery probability than B<sub>E</sub> (described below).



*You can view the amount of traffic on the selected physical interface which is marked as discard eligible via the Frame Relay Congestion Stats window, described beginning on [page 5-22](#).*

### **B<sub>E</sub> (In/Out)**

Use this field to enter the Excess Burst Size (B<sub>E</sub>) assigned to the selected DLCI by your frame relay provider. The excess burst size defines the amount of data (in bits) *over* the committed burst size (B<sub>C</sub>) that the network will attempt to transfer during the time interval T<sub>C</sub> (remember, T<sub>C</sub> is calculated by dividing the committed burst size (B<sub>C</sub>) by the committed information rate (CIR)). Any data exceeding this value will be buffered in the FRX device. Note that DE frames are considered to be B<sub>E</sub> excess data.

### **BECN**

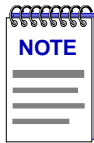
The BECN Recovery Count provides a means for controlling the rate of return to maximum traffic flow after it has been reduced due to congestion. If a packet is *received* on the selected DLCI with the BECN (backward explicit congestion notification) bit set, the configured **B<sub>E</sub> Out** value will be ignored and the effective value will become zero (limiting traffic flow to the value configured for **B<sub>C</sub> Out**). This limit will remain in place until the DLCI receives a specified number of sequential packets without the BECN bit set: the number specified by the BECN Recovery Count. Each time the configured number of sequential packets is received, the effective **B<sub>E</sub> Out** will be increased by one-eighth of the configured value.

**Priority**

The Outgoing DLCI Priority value allows you to assign relative priority levels to the DLCIs configured on the selected physical port. The allowable range is 0-4, with 0 being the lowest priority.

**Backup Group Number**

Use this field to specify whether this DLCI is a primary or a backup DLCI. If it is a primary DLCI, enter the number (1-255) that identifies the Frame Relay Backup Group that will take over if this DLCI fails. If it is a backup DLCI, enter 0. A DLCI cannot be both a backup and a primary DLCI.



*If you are configuring a primary DLCI, you must set this value to 0 until you have configured a Frame Relay Backup Group (see [Configuring a Frame Relay Backup Group, page 5-13](#)). Then, re-access the Frame Relay DLCI Table and specify the desired backup group.*

This parameter is applicable only on an initiating node, which is the node that will initiate the switchover to a backup DLCI. At switchover, the initiating node notifies the remote (non-initiating) node of the change. Do **not** configure a Backup Group Number on this DLCI at the remote (non-initiating) end.

**Backup Protocol**

This field is only configurable if the Backup Group Number is set to 0, indicating that the DLCI being configured is a backup DLCI. Set this field to Enabled if this DLCI will be used as a remote (non-initiating) backup. The DLCI will wait for a backup protocol message from the initiating end, telling the backup where to send the rest of the messages. Set this field to Disabled if this DLCI is an initiating backup.

**State**

Although it appears to be a settable parameter, the value displayed in the State field simply indicates the internal status of the entry you are configuring: active, inactive, or invalid. The value displayed here indicates only the device's efforts to add the entry to its MIB table.

**Changing DLCI Rate Values**

To edit the rate values assigned to each configured DLCI:

1. If you wish to modify an existing entry, be sure that entry is highlighted in the list box portion of the window.
2. Enter and/or edit the values displayed in the text boxes, as desired. (Remember, some values which are settable from this window must mirror values received from your service provider or configured elsewhere; be sure these values match as necessary.)

3. Click on **Add** to create a new entry, or on **Modify** to edit the entry currently selected in the list box.

### Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

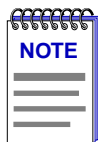
## Frame Relay Backup Groups

Frame Relay Backup Groups provide frame relay DLCIs with automatic backup protection should a DLCI fail. DLCIs are configured as either “primary” DLCIs or “backup” DLCIs. This is done either in console management (refer to your FRX or SmartSwitch 1800 hardware documentation) or in the Frame Relay DLCI Rate Configuration window (see [DLCI Rate Configuration](#), page 5-8).

In a backup configuration, one end of the link is considered the “initiating” node and the other is the “remote”, or non-initiating, node. The initiating end is the node that will establish the backup DLCI if it discovers that the primary DLCI is down. A node can be the initiating node for some backup configurations, and the remote node for others.

On the initiating node, backup DLCIs are assigned to backup groups. Each group can contain up to ten backup DLCIs. A backup group is then assigned to one or more primary DLCI; each DLCI can have just one backup group.

If a node detects a failure in a primary DLCI connection, it will search the backup group assigned to that primary DLCI, and will select the first available DLCI in that group as a backup. The backup will become operational and will remain in that state until the primary becomes active again. If the backup fails while in use, the node will check the status of the primary, then (if necessary) search the primary’s backup group for another backup.



*Any sessions in progress when a primary DLCI goes down will not be transferred directly to the backup DLCI, but will be reset, then established on the backup.*

Before configuring Frame Relay Backup Groups, you should first configure all the primary and backup DLCIs using either console management (refer to your FRX or SmartSwitch 1800 hardware documentation) or the Frame Relay DLCI Rate Configuration window (see [DLCI Rate Configuration](#), page 5-8). All DLCI

parameters can be configured, except specifying a Backup Group Number for the primary DLCI on the initiating node. The next step is to configure your Backup Groups using the information in this section. You can then return to your DLCI configuration and enter the appropriate Backup Group Number that will assign a backup group to each primary DLCI.

## Configuring Frame Relay Backup Groups

Use the Frame Relay Backup Groups window to configure backup groups. To access the window:

1. Click on the **Device** button to display the Device menu.
2. Drag down to **Frame Relay Backup Group**, and release. The Frame Relay Backup Group window, [Figure 5-3](#), will appear.

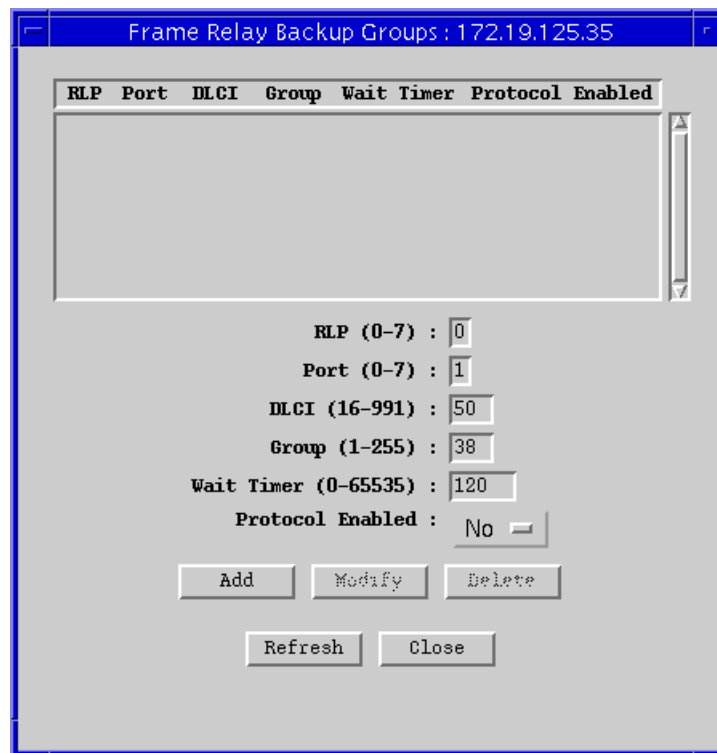


Figure 5-3. Frame Relay Backup Group

The list box at the top of the window displays each backup DLCI and the group it is assigned to; the fields and buttons in the lower portion of the window allow you to add new entries and modify or delete existing ones.

Each backup DLCI is configured using the following parameters:

**RLP**

Indicates the RLP where the physical port on which the backup DLCI is being configured resides. For the FRX4000 and SmartSwitch 1800 this would always be 0. For the FRX6000 this could be RLP 0 - 7.

**Port**

Indicates the physical port on which the backup DLCI is being configured.

**DLCI**

This is the DLCI number of the backup being configured. The DLCI must already have been created either in console management (refer to your FRX or SmartSwitch 1800 hardware documentation) or in the Frame Relay DLCI Rate Configuration window (see [DLCI Rate Configuration](#), page 5-8).

**Group**

Defines the frame relay backup group the backup DLCI belongs to. A backup group is then assigned to one or more primary DLCIs.

Each backup group can contain up to ten backup DLCIs. A DLCI cannot be assigned to more than one backup group, nor can it be assigned to a backup group if it is a primary DLCI (one that will be backed up).

**Wait Timer**

Indicates the time (in seconds) after a primary DLCI failure that the initiating node will wait for this backup DLCI to become active before checking the next backup DLCI. If the backup DLCI does not become active before the timer expires, the node will search the backup group for the next available backup.

**Protocol Enabled**

If **Yes** is selected, the backup protocol on the specified DLCI is enabled. This field should be set to **Yes** if, and only if, the remote node is a FRX or SmartSwitch 1800 with the backup protocol enabled on the remote DLCI connected to this backup group entry.

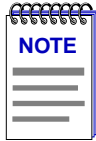
The remote node must be the same one to which the primary DLCI was connected, and the remote node's backup DLCI must be on the same RLP as its primary DLCI. Also, the primary DLCI in the initiating node must have the remote node's primary RLP, port, and DLCI configured in its DLCI parameters.

## Changing Backup Group Values

To edit the values assigned to each backup DLCI:

1. If you wish to modify an existing entry, be sure that entry is highlighted in the list box portion of the window.
2. Enter and/or edit the values displayed in the text boxes, as desired. (Remember, some values which are settable from this window must mirror values received from your service provider or configured elsewhere; be sure these values match as necessary.)

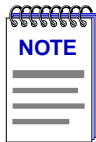
3. Click on **Add** to create a new entry, or on **Modify** to edit the entry currently selected in the list box.



*After you have made system-level changes (such as configuring Frame Relay Backup Groups), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Configuring Logical Ports

A frame relay port can contain multiple logical ports, allowing multiple protocols to run over a single physical frame relay port. You can configure up to 56 logical ports in an FRX4000 or SmartSwitch 1800, and up to 56 logical ports per RLP in an FRX6000. All 56 logical ports can reside on one physical port, or be spread over several physical ports.



*Before configuring a logical port, make sure the physical frame relay port on which the logical port will reside has been configured. Refer to [Configuring Frame Relay Ports](#), page 5-2.*

Using the Logical Port Configuration window, you can configure some basic operational parameters for each of your logical ports.

To access the window:

1. Click mouse button 3 on the frame relay port of interest to display the Port Menu.
2. Drag down to **Logical Port Configuration**, and release. The Logical Port Configuration window, [Figure 5-4](#), will appear.

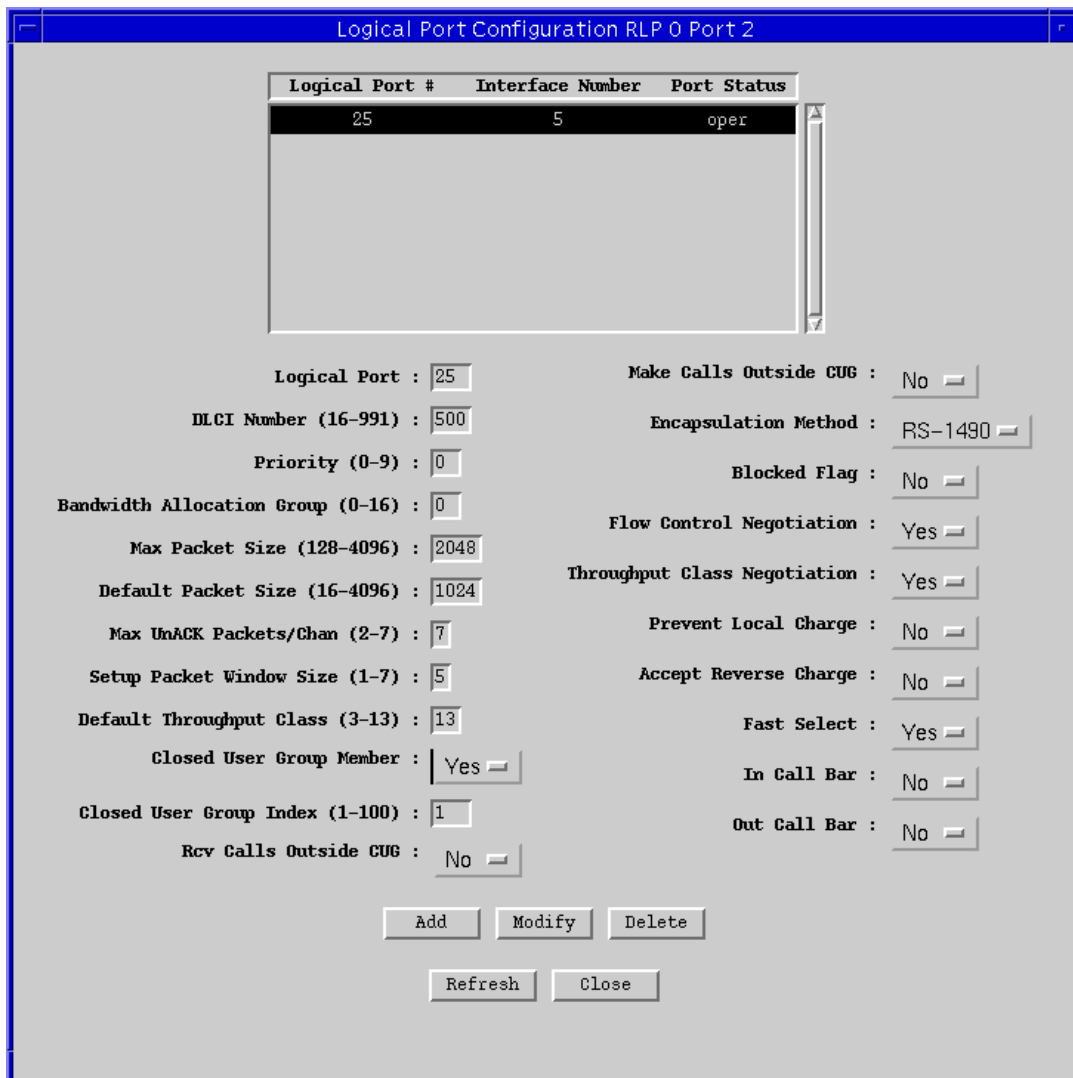


Figure 5-4. Logical Port Configuration

The Logical Port Configuration window allows you to configure the following parameters:

**Logical Port**

This field specifies the number of the logical port being configured. Valid entries are 8 - 63.

**DLCI Number**

Use this field to enter the Data Link Connection Identifier (DLCI), a routing ID that links the logical port to a virtual connection on the physical frame relay port. This number is usually assigned by your frame relay provider.



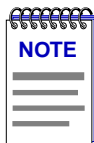
You must configure a different DLCI for every logical port on a physical port because logical ports and DLCIs have a one-to-one relationship. Also, make sure that each interface (IP, IPX or LLC2) or frame relay bridge port has a different DLCI. Do not assign a DLCI number that is configured as a frame relay backup DLCI.

### Priority

This field allows you to set a priority for traffic within the node. The higher the number, the higher the priority relative to other intra-nodal traffic. These priorities have no effect on traffic exiting a node. When configuring priorities, be careful to consider the types of traffic being routed on other connections in the node.

### Bandwidth Allocation Group

Use this field to assign the logical port to one of 16 Bandwidth Allocation Groups (BAG). BAGs regulate bandwidth usage by outgoing traffic on the physical link and can ensure that response time-sensitive traffic gets access to the available frame relay bandwidth. Up to 16 groups can be defined and configured through console management (refer to your FRX or SmartSwitch 1800 hardware documentation for more information).



*Bandwidth allocation groups cannot currently be configured via SPMA; for more information on configuring these groups, see your FRX or SmartSwitch 1800 hardware documentation.*

### Max Packet Size

Use this field to specify the maximum data packet size that will be allowed to pass through this logical port. The packet size included in a call setup packet will be used, as long as it is smaller than the maximum specified here. Valid values are 128, 256, 512, 1024, 2048 and 4096.

If X.25 will be run over this port, do not configure a size greater than 2048. If 4096 is specified, additional X.25 and frame headers can make the frame too large. The value of 2048 will not cause a problem, since larger frames will simply be split, then reassembled at the destination.

### Default Packet Size

The value entered in this field will be assigned to an incoming call setup packet if the packet does not include a packet size. Valid values are 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096.

If X.25 will be run over this port, do not configure a size greater than 2048. If 4096 is specified, additional X.25 and frame headers can make the frame too large. The value of 2048 will not cause a problem, since larger frames will simply be split, then reassembled at the destination.

### Max UnACK Packets/Channel

This specifies the maximum number of sequentially numbered frames that can be waiting for acknowledgment by the destination device. If this number is exceeded, no frames will be transmitted until an acknowledgment is received.

### Setup Packet Window Size

This specifies a default window size that will be assigned to an incoming call setup packet if the packet does not include a window size. Valid values are 1 to 7 packets.

### Default Throughput Class

Use this field to specify the value that will be inserted into a Call Request packet if **Throughput Class Negotiation** is not enabled or if a throughput class is not requested in the Call Request. This value should not be higher than the line speed specified for the physical port.

Enter a number 3 - 13 that corresponds to the following values (in bits per second):

3 = 75	7 = 1200	11 = 19.2K
4 = 150	8 = 2400	12 = 48K
5 = 300	9 = 4800	13 = 64K
6 = 600	10 = 9600	

### Closed User Group Member

This field specifies whether the port belongs to a Closed User Group (CUG). The CUG function is a privacy feature that allows the creation of up to 100 groups of users per port. Members of a CUG can communicate with other members, but access to and from network users outside that CUG may be denied (determined by **Rcv Calls Outside CUG** and **Make Calls Outside CUG**).



*Closed User Groups (CUG) are configured using console management. Refer to your FRX or SmartSwitch 1800 hardware documentation for more information about CUGs*

### Closed User Group Index

This field is only configurable if the port is a CUG member; it specifies which Closed User Group the port belongs to. The CUG index number is included in call packets, and is cross-referenced with the CUG Index created through console management.

### Rcv Calls Outside CUG

This field is only configurable if the port is a CUG member; it specifies whether the logical port can receive calls from network users outside that CUG.

### Make Calls Outside CUG

This field is only configurable if the port is a CUG member; it specifies whether the logical port can make calls to network users outside that CUG.

### Encapsulation Method

This field specifies whether the traffic will be encapsulated by Annex G or RS 1490 for transmission across the frame relay network.

With Annex G, an LAPB frame is encapsulated immediately following the frame relay header (flag, 2-byte T1.618 header, LAPB address, LAPB control, LAPB I-field, [x.25/x.75]). With RFC 1490, the order is: T1.618 header, Q.922 control byte, Q.933 NLPID, 2-byte level-2 protocol ID, 2-byte level-3 protocol ID, LAPB frame.

- RFC 1490 — The protocols will be identified on the DLCI based on their NLPIDs and (if applicable) level-2 and level-3 headers (e.g., X.25: flag, T1.618 2-byte header, 0x03 Q.922 control, 0x08 Q.933 NLPID, T1.617 level-2 LAPB PID 0x51 81, T1.617 level-3 PID 0x67 80, LAPB frame).
- Annex G — Each protocol must be encapsulated in X.25 for transmission over a single DLCI, because Annex G allows the DLCI to be used only by X.25. Each protocol would require its own X.25 virtual circuit and level-3 window.

### Blocked Flag

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or re-booted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed.

### Flow Control Negotiation

This field allows for negotiation of flow control parameters (packet and window sizes for data transmission in either direction) on a per-call basis. If **No** is selected, the **Default Packet Size** and **Setup Packet Window Size** will be used. If **Yes** is selected, a packet and/or window size included in a call packet will be used. (If a packet and/or window size is not included, the default values will be used.)

### Throughput Class Negotiation

This field allows for negotiation of throughput classes for data transmission in either direction on a per-call basis. If **No** is selected, the **Default Throughput Class** will be used. If **Yes** is selected, any throughput class included in a call packet will be used. (If a throughput class is not included, the default value will be used.)

### Prevent Local Charge

This field is used to prevent calls from being charged to this port. If **Yes** is selected, incoming calls from the network with Reverse Charging specified will be rejected and outgoing calls will have Reverse Charging inserted if it is not already in the call packet. If **No** is selected, then calls can be charged to this port.

#### **Accept Reverse Charge**

This field is used to authorize the transmission of incoming calls that request Reverse Charging. If **Yes** is selected, a call requesting Reverse Charging will be accepted. If **No** is selected, and a call requests Reverse Charging, the call will not be transmitted.

#### **Fast Select**

This field authorizes transmission of incoming calls that request the X.25 Fast Select facility.

#### **In Call Bar**

This is an X.25 facility that prevents the transmission of incoming calls to this port.

#### **Out Call Bar**

This is an X.25 facility that prevents the transmission of outgoing calls from this port.

## Changing Configuration Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.

If you have made changes to the fields but would like to revert back to the previous values, click on the **Refresh** button.

3. Click on  to save your changes.

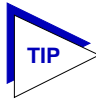
## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## Viewing Frame Relay Status

Three additional port-level menu selections provide statistical information regarding frame relay traffic and performance on a selected port.



The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.

## Management Stats

The Management Statistics window provides general information about the type of management traffic that is being transmitted across the selected port. To access the window:

1. Click mouse button 3 on the frame relay port of interest to display the Port Menu.
2. Drag down to **Frame Relay Management Stats**, and release. The Frame Relay Management Statistics window, [Figure 5-5](#), will appear.

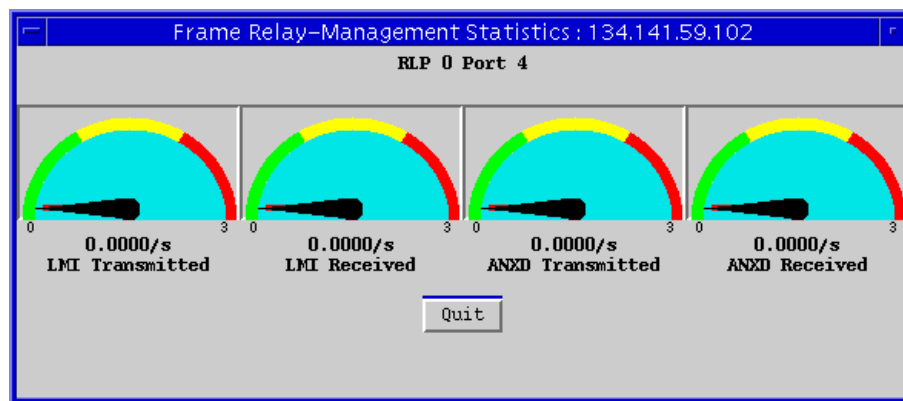


Figure 5-5. Frame Relay Management Stats

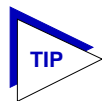
The Management Stats window provides the following statistical data:

### **LMI (Transmitted and Received)**

Displays the number of management frames using LMI (link management interface) rev1 format that were transmitted or received across the selected port, expressed as a rate (frames/second).

### **ANXD (Transmitted and Received)**

Displays the number of management frames using ANSI-defined Annex D format that were transmitted or received across the selected port, expressed as a rate (frames/second).



You can select the type of management frames that will be transmitted across a selected port by configuring the Link Layer Management option in the Frame Relay Port Configuration window, described beginning on [page 5-2](#).

## Congestion Stats

The Congestion Statistics window provides information about the rates at which Discard Eligible and Congestion Notification frames are being both received and transmitted. To access the window:

1. Click mouse button 3 on the frame relay port of interest to display the Port Menu.
2. Drag down to **Frame Relay Congestion Stats**, and release. The Frame Relay Congestion Statistics window, [Figure 5-6](#), will appear.

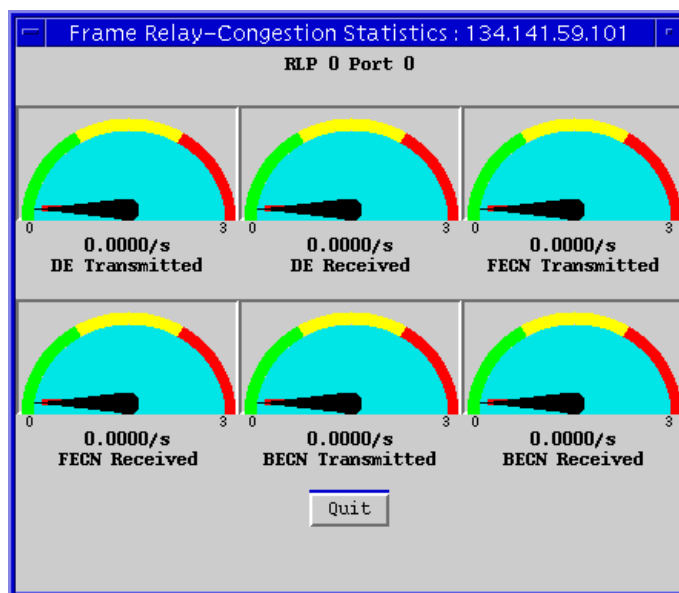


Figure 5-6. Frame Relay Congestion Stats

The Congestion Statistics window provides the following statistical data:

### DE (Transmitted and Received)

Displays the number of frames with the discard eligible (DE) bit set that were transmitted or received on the selected port, expressed as a rate (frames/second). Traffic which exceeds the configured CIR and/or  $B_C$  parameters will be marked as discard eligible. (See [page 5-9](#) and following for more information on these values.)

**BECN (Transmitted and Received)**

Displays the number of frames with the BECN (backward explicit congestion notification) bit set that were transmitted or received on the selected port, expressed as a rate (frames/second). BECN frames notify the user that traffic sent in the opposite direction to the received frame may encounter a congested path; this alerts the device to reduce inbound traffic.

**FECN (Transmitted and Received)**

Displays the number of frames with the FECN (forward explicit congestion notification) bit set that were transmitted or received on the selected port, expressed as a rate (frames/second). FECN frames notify the receiving device that the frames have been delivered through a congested network path; this alerts the destination device to slow its transmission rate.

**Errors**

The Error Statistics window displays the rate at which frames are being discarded at the selected port. To access the window:

1. Click mouse button 3 on the frame relay port of interest to display the Port Menu.
2. Drag down to **Frame Relay Errors**, and release. The Frame Relay Errors window, [Figure 5-7](#), will appear.

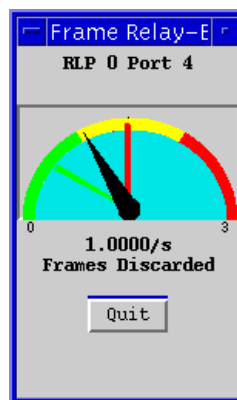


Figure 5-7. Frame Relay Errors

The Errors window provides a single meter displaying the following statistic:

**Frames Discarded**

Displays the number of incoming and outgoing frames discarded due to congestion, expressed as a rate (frames/second).





# X.25 Status and Configuration

*About using the X.25 protocol; configuring X.25 ports; viewing X.25 management, congestion, and error stats*

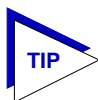
---

An FRX or SmartSwitch 1800 port configured to run X.25 as its layer 2 protocol can connect to an X.25 DTE or an X.25 network. This allows the port to transmit X.25 traffic, as well as IP and IPX traffic (encapsulated as per RFC 1356) and SNA traffic. For any FRX or SmartSwitch 1800 physical ports which have been configured to use X.25 as their layer 2 protocol (that is, those which display a Port Type of X25), SPMA provides a variety of statistical information.

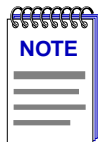
For each physical port configured to run X.25, one configuration window and three statistical windows are provided:

- The **X.25 Physical Port Configuration** window allows you to configure basic operational parameters related to the X.25 protocol;
- **X.25 Management Stats** provide management information about standard LAPB command and response frames, displayed via meters;
- **X.25 Congestion Stats** provide information about standard LAPB command and response frames related to the level of traffic present, displayed in meters; and
- The **X.25 Errors** window provides information about standard LAPB command and response frames related to error conditions, also displayed in meters.

These windows and their functions are described in the following sections.



*The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.*



Note that a frame relay port can support encapsulated X.25 traffic on a logical port. For information on logical ports, see Chapter 5.

## Configuring X.25 Physical Ports

The X.25 Physical Port Configuration window allows you to set X.25 operational parameters for physical ports.

To access the window:

1. Click mouse button 3 on the X.25 port of interest to display the Port Menu.
2. Drag down to **X.25 Physical Port Configuration**, and release. The X.25 Physical Port Configuration window, [Figure 6-1](#), will appear.

Parameter	Value	Parameter	Value
Speed	64000	Connector Type	RS-232
Inactivity Timer (1-30)	5	Dial In/Out	None
Disconnect Timer (1-255)	5	Generate Clock	Yes
Setup Timer (1-255)	5	Receive Clock From DTE	No
Max Packet Size (128-4096)	1024	Network Trunk Group	No
Default Packet Size (16-4096)	128	Blocked Flag	No
Max UnACK Packets/Chan (2-7)	7	Flow Control Negotiation	No
Setup Packet Window Size (1-7)	2	Throughput Class Negotiation	No
Default Throughput Class (3-13)	10	Prevent Local Charge	No
Closed User Group Member	Yes	Accept Reverse Charge	No
Closed User Group Index (1-100)	1	Fast Select	No
Rcv Calls Outside CUG	No	In Call Bar	No
Make Calls Outside CUG	No	Out Call Bar	No

Buttons: Apply, Close

Figure 6-1. X.25 Physical Port Configuration

The X.25 Physical Port Configuration window provides the following configuration information:

### Speed

This field specifies the data transmission rate in bits per second. If this port is a physical DTE, specify the line speed that matches the speed of the device connected directly to the port. If the port is a physical DCE (i.e., the attached I/O cable is DCE) specify the clock speed of the serial port you are configuring.

Possible line speed entries are:

75	64000	512000	1008000	1472000
150	72000	560000	1024000	1512000
300	112000	576000	1064000	1536000
600	128000	616000	1088000	1568000
1200	168000	640000	1120000	1600000
2400	192000	672000	1152000	1624000
4800	224000	704000	1176000	1664000
9600	256000	728000	1216000	1668000
14400	280000	768000	1232000	1728000
19200	320000	784000	1280000	1792000
24000	336000	832000	1288000	1856000
28800	384000	840000	1344000	1920000
38400	392000	896000	1400000	1984000
48000	448000	952000	1408000	2048000
56000	504000	960000	1456000	

If you enter a value that is within the valid range but not equal to one of the values listed above, the speed will be rounded up. If an RS-232 DCE port is directly connected to the DTE via the standard Cabletron cable, the maximum supported speed is 64000. If longer cabling is used, the maximum speed is 19200.

### Inactivity Timer

The Inactivity Timer only has a function if the port you are configuring is a dial port; that is, if the port is connected to a dial modem. Use this field to specify an amount of time (in minutes) that starts as soon as there are no active connections on a dial port. If the port is a dial-out port, and no new connections are established before the specified time expires, the port will be disabled until the next call is placed. If the port is a dial-in port, and no new connections are established before the time period expires, the port will be disabled until the **Disconnect Timer** expires.

### Disconnect Timer

The Disconnect Timer only has a function if the port you are configuring is a dial port; that is, if the port is connected to a dial modem. This field specifies the length of time (in seconds) that a dial-in port will remain disabled after the **Inactivity Timer** expires.

### Setup Timer

The Setup Timer only has a function if the port you are configuring is a dial port; that is, if the port is connected to a dial modem. The setup timer starts when the port enters the linkup state. Use this field to enter a time period (in seconds). If there is no response from the other end before the time period expires, the port will enter the failed state.

### Max Packet Size

Use this field to specify the maximum data packet size that will be allowed to pass through this X.25 port. The packet size included in a call setup packet will be used, as long as it is smaller than the maximum specified here. Valid values are 128, 256, 512, 1024, 2048, and 4096.

### Default Packet Size

The value entered in this field will be assigned to an incoming call setup packet if the packet does not include a packet size. Valid values are 16, 32, 64, 128, 256, 512, 1024, 2048, and 4096.

### Max UnACK Packets/Channel

This specifies the maximum number of sequentially numbered frames that can be waiting for acknowledgment by the destination device. If this number is exceeded, no frames will be transmitted until an acknowledgment is received.

### Setup Packet Window Size

This specifies a default window size that will be assigned to an incoming call setup packet if the packet does not include a window size. Valid values are 1 to 7 packets.

### Default Throughput Class

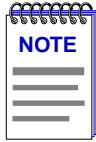
Use this field to specify the value that will be inserted into a Call Request packet if **Throughput Class Negotiation** is not enabled or if a throughput class is not requested in the Call Request. This value should not be higher than the line speed specified for the physical port.

Enter a number 3 - 13 that corresponds to the following values (in bits per second):

3 = 75	7 = 1200	11 = 19.2K
4 = 150	8 = 2400	12 = 48K
5 = 300	9 = 4800	13 = 64K
6 = 600	10 = 9600	

### Closed User Group Member

This field specifies whether the port belongs to a Closed User Group (CUG). The CUG function is a privacy feature that allows the creation of up to 100 groups of users per port. Members of a CUG can communicate with other members, but access to and from network users outside that CUG may be denied (determined by **Rcv Calls Outside CUG** and **Make Calls Outside CUG**).



*Closed User Groups (CUG) are configured using console management. Refer to your FRX or SmartSwitch 1800 hardware documentation for more information about CUGs*

### **Closed User Group Index**

This field is only configurable if the port is a CUG member; it specifies which Closed User Group the port belongs to. The CUG index number is included in call packets, and is cross-referenced with the CUG Index created through console management.

### **Rcv Calls Outside CUG**

This field is only configurable if the port is a CUG member; it specifies whether the logical port can receive calls from network users outside that CUG.

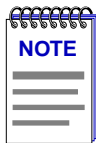
### **Make Calls Outside CUG**

This field is only configurable if the port is a CUG member; it specifies whether the logical port can make calls to network users outside that CUG.

### **Connector Type**

This field is defined by the port's connector and cabling type, and must be configured as follows:

- For the FRX4000 and SmartSwitch 1800, port 0 and port 1 are always RS-232;



*If you have installed the optional CSU/DSU card on an FRX4000 or SmartSwitch 1800, it will logically take port 1, and you must configure certain CSU/DSU parameters through console management. Refer to your FRX or SmartSwitch 1800 hardware documentation for more information.*

- For the FRX4000, ports 2 and 3 are determined by the attached cables: RS-232, V.35, RS-449, or X.21;
- For the SmartSwitch 1800, ports 2 and 3 are determined by the attached cables: RS-232, V.35, or RS-449;
- For the FRX4000, ports 4-7 are determined by the expansion Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, and X.21. (RS-449 and X.21 interfaces require an RS-422 LIC.)
- For the FRX6000, ports 0-7 on each RLP are determined by the Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, RS-530 and X.21. (RS-449, RS-530, and X.21 interfaces require an RS-422 LIC.)

### Dial In/Out

This parameter only has a function if the port you are configuring is a dial port; that is, if the port is connected to a dial modem. It specifies whether this port is connected to a dial modem and, if so, whether connections will be initiated through dial-in or dial-out calls. (Signaling differences prevent configuration for both dial-in and dial-out on the same port.)

A port specified as **Dial Out** will establish a link only when an outgoing X.25 call is placed, at which time the port will raise DTR (Data Terminal Ready) and the attached modem will dial a stored number to a remote modem to establish an X.25 connection. A port specified as **Dial In** will establish a link only when a call is received.

If the port is configured as a network trunk (see **Network Trunk Group** below), the value must be **None**.

### Generate Clock

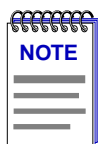
This field specifies whether the port will generate the clock necessary to synchronize traffic over the link. If the port is a physical DCE (determined by the port's I/O cable interface), configure this field as **Yes**, since the physical DCE generates clock. If the port is a DTE, configure this field as **No**.

### Receive Clock from DTE

This parameter is relevant only if **Connector Type** is something other than RS-232, and the **Generate Clock** parameter is set to **Yes** (see above). Selecting **Yes** for this field allows the clock to be looped back from the DTE using the TT (Terminal Timing) signal, which can be helpful on high-speed lines. Generally, if the local interface is physical DCE and the line speed is above 256 Kbps, this parameter should be set to **Yes**. (Make sure the remote DTE is configured to provide the terminal timing.)

### Network Trunk Group

A network trunk is a link between FRX and SmartSwitch 1800 devices over X.25. You can assign a port to a trunk group which will cause that port to be enabled when the network trunk is operational, or disabled if the network trunk is not operational.



*Although you can use this window to designate an X.25 port as a member of a trunk group, you must configure the actual network trunk through console management. Refer to your hardware documentation for more information on network trunks.*

### Blocked Flag

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or re-booted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed.

### **Flow Control Negotiation**

This field allows for negotiation of flow control parameters (packet and window sizes for data transmission in either direction) on a per-call basis. If **No** is selected, the **Default Packet Size** and **Setup Packet Window Size** will be used. If **Yes** is selected, a packet and/or window size included in a call packet will be used. (If a packet and/or window size is not included, the default values will be used.)

### **Throughput Class Negotiation**

This field allows for negotiation of throughput classes for data transmission in either direction on a per-call basis. If **No** is selected, the **Default Throughput Class** will be used. If **Yes** is selected, any throughput class included in a call packet will be used. (If a throughput class is not included, the default value will be used.)

### **Prevent Local Charge**

This field is used to prevent calls from being charged to this port. If **Yes** is selected, incoming calls from the network with Reverse Charging specified will be rejected and outgoing calls will have Reverse Charging inserted if it is not already in the call packet. If **No** is selected, then calls can be charged to this port.

### **Accept Reverse Charge**

This field is used to authorize the transmission of incoming calls that request Reverse Charging. If **Yes** is selected, a call requesting Reverse Charging will be accepted. If **No** is selected, and a call requests Reverse Charging, the call will not be transmitted.

### **Fast Select**

This field authorizes transmission of incoming calls that request the X.25 Fast Select facility. This field must be set to **Yes** if SDLC-LLC2 conversion is configured over the port, or if the X.25 link is to an X.25 network.

### **In Call Bar**

This is an X.25 facility that prevents the transmission of incoming calls to this port.

### **Out Call Bar**

This is an X.25 facility that prevents the transmission of outgoing calls from this port.

## Changing Configuration Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.

If you have made changes to the fields but would like to revert back to the previous values, click on the **Refresh** button.

3. Click on  to save your changes.

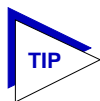
## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## Viewing X.25 Status

For each physical port configured to run X.25, three statistical windows are provided. These windows provide traffic and performance information for the selected port; they are described in the following sections.



*The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.*

## Management Stats

The Management Statistics window provides information about standard LAPB command and response frames related to management actions taken at the selected port. To access the window:

1. Click mouse button 3 on the X.25 port of interest to display the Port Menu.
2. Drag down to **X25 Management Stats**, and release. The X25 Management Statistics window, [Figure 6-2](#), will appear.



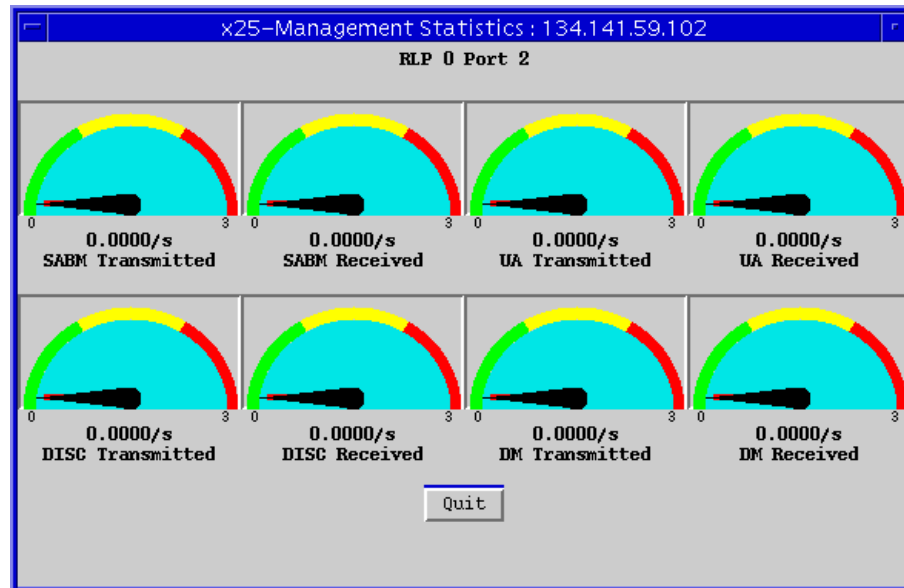


Figure 6-2. X.25 Management Stats

The Management Statistics window provides the following statistical data:

**SABM (Transmitted/Received)**

A count of the Set Asynchronous Balanced Mode (SABM) commands transmitted or received across the selected port, expressed as a rate (commands/second).

**UA (Transmitted/Received)**

A count of the Un-numbered Acknowledgment (UA) responses transmitted or received across the selected port, expressed as a rate (responses/second).

**DISC (Transmitted/Received)**

A count of the Disconnect (DISC) commands transmitted or received across the selected port, expressed as a rate (commands/second).

**DM (Transmitted/Received)**

A count of the Disconnect Mode (DM) responses transmitted or received across the selected port, expressed as a rate (responses/second).

## Congestion Stats

The Congestion Statistics window provides information about standard LAPB command and response frames related to the level of traffic present on the selected port. To access the window:

1. Click mouse button 3 on the X.25 port of interest to display the Port Menu.

2. Drag down to **X25 Congestion Stats**, and release. The X25 Congestion Statistics window, [Figure 6-3](#), will appear.

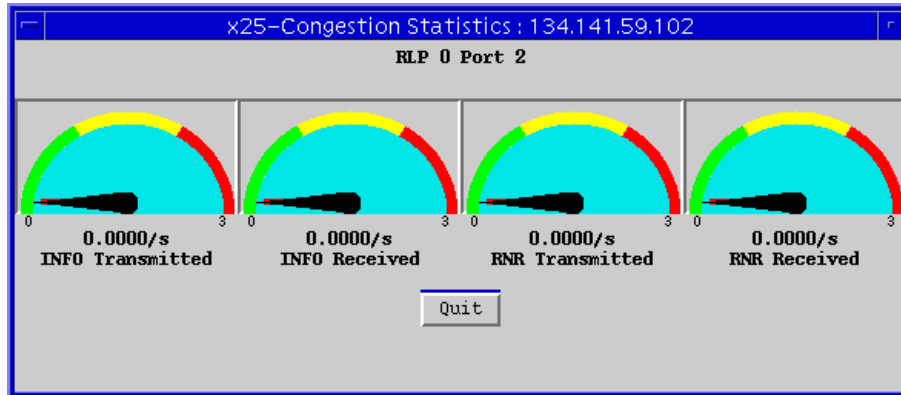


Figure 6-3. X.25 Congestion Stats

The Congestion Statistics window provides the following statistical data:

**INFO (Transmitted/Received)**

A count of the Information Transfer (INFO) commands transmitted or received across the selected port, expressed as a rate (commands/second).

**RNR (Transmitted/Received)**

A count of the Receive Not Ready (RNR) supervisory commands or responses transmitted or received across the selected port, expressed as a rate (commands or responses/second).

## Errors

The Error Statistics window provides information about standard LAPB command and response frames related to error conditions present on the selected port. To access the window:

1. Click mouse button 3 on the X.25 port of interest to display the Port Menu.
2. Drag down to **X25 Errors**, and release. The X25 Error Statistics window, [Figure 6-4](#), will appear.

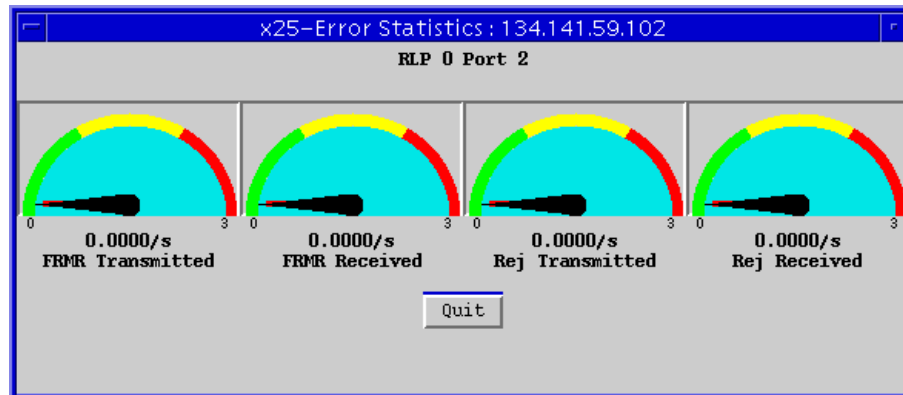


Figure 6-4. X.25 Error Stats

The Error Statistics window provides the following statistical data:

**FRMR (Transmitted/Received)**

A count of the Frame Reject (FRMR) responses transmitted or received on the selected port, expressed as a rate (responses/second).

**Rej (Transmitted/Received)**

A count of the Reject (Rej) supervisory commands or responses transmitted or received on the selected port, expressed as a rate (commands or responses/second).



# SNA Status and Configuration

*Configuring SNA ports; physical unit and LLC2 parameter configuration; configuring link stations; configuring LLC2 hosts; viewing statistics*

---

SNA ports in the FRX4000, FRX6000, and SmartSwitch 1800 connect IBM hosts with PUs (physical units), over a frame relay (via RFC 1490) or X.25 (via Annex G) network. SNA support includes SDLC (Synchronous Data Link Control) for serial lines and LLC2 (Logical Link Control type 2) for LAN connections. SDLC-to-LLC2 and LLC2-to-SDLC conversion is performed for transmission over frame relay.

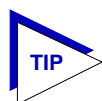
For each physical port configured to run SNA, six configuration windows are provided:

- The **SDLC Port Configuration** window allows you to configure the SNA port that will connect to user devices;
- The **SDLC PU Configuration** window, where you define the physical units (PU) that will communicate via the SNA port;
- The **SDLC PU LLC2 Configuration** window, where you configure the physical unit's LLC2 parameters (if SDLC-LLC2 conversion will be performed on the PU connection);
- The **SDLC Link Station Configuration** window allows you to configure the SDLC link stations;
- The **SNA/LLC2 Hosts Table** where each SNA/LLC2 host device is configured;
- The **LLC2 Hosts Connections Tables** where LLC2 Host connections are configured.

In addition, for each SNA port there are four statistical windows provided:

- The **SDLC Port Stats** providing general port statistics;
- The **SDLC LS General Stats** providing link station statistics;
- The **SDLC LS Rx Stats** providing link station receive statistics;
- The **SDLC LS Tx Stats** providing link station transmit statistics.

These windows and their functions are described in the following sections.



*The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.*

## Configuring SNA Ports

Each SNA port can be configured to support SNA hosts (PU 2.1, 4.0 HPAD, or NPAD) or terminals (PU 1.0, 2.0, 2.1 TPAD). A port can also be configured for a transparent mode (XPAD), which supports HDLC (High-level Data Link Control) and any of its subset protocols, such as SDLC, LAPB (Link Access Procedure), and BSC (Binary Synchronous Communications).

### SDLC Port Configuration

Using the SDLC Port Configuration window, you can configure the SNA port that will connect to the user devices, if the connection will be SDLC.

To access the window:

1. Click mouse button 3 on the SNA port of interest to display the Port Menu.
2. Drag down to **SDLC Port Configuration**, and release. The SDLC Port Configuration window, [Figure 7-1](#), will appear.

The screenshot shows a configuration window titled "SDLC Config. RLP 0 Port 2". It contains the following settings:

- Packet Size (16-4096) : 1024
- Line Speed : 9600
- MAX Retries (0-99) : 5
- MAX Out (1-7) : 7
- Inactivity Timer (15-250) : 50
- Physical Port Interface : RS-232
- PAD Type : xpad
- LPDA Support : None
- NRZ Data Encoding : No
- Generate Clock : No
- Recv Clock from DTE : No
- Disable Rqst Disconnect : No
- Idle Fill Char : hex-ff
- L1 Duplex : Full

At the bottom of the window are two buttons: "Apply" and "Close".

Figure 7-1. SDLC Port Configuration

The SDLC Port Configuration window provides the following information:

**Packet Size**

This field specifies the maximum packet size (in bytes) that will be transmitted on the port. The default value for this parameter is 1024.

**Line Speed**

This field specifies the data transmission rate in bits per second. If this port is a physical DTE, specify the line speed that matches the speed of the device connected directly to the port. If the port is a physical DCE (i.e., the attached I/O cable is DCE) specify the clock speed of the serial port you are configuring.

Possible line speed entries are:

75	64000	512000	1008000	1472000
150	72000	560000	1024000	1512000
300	112000	576000	1064000	1536000
600	128000	616000	1088000	1568000
1200	168000	640000	1120000	1600000
2400	192000	672000	1152000	1624000
4800	224000	704000	1176000	1664000
9600	256000	728000	1216000	1668000
14400	280000	768000	1232000	1728000
19200	320000	784000	1280000	1792000
24000	336000	832000	1288000	1856000
28800	384000	840000	1344000	1920000
38400	392000	896000	1400000	1984000
48000	448000	952000	1408000	2048000
56000	504000	960000	1456000	

If you enter a value that is within the valid range but not equal to one of the values listed above, the speed will be rounded up. If an RS-232 DCE port is directly connected to the DTE via the standard Cabletron cable, the maximum supported speed is 64000. If longer cabling is used, the maximum speed is 19200.

#### MAX Retries

This is the maximum number of times the port will attempt to send a frame if the physical unit (PU) is not responding. A larger value increases the probability of an eventual correct transfer between DTE and DCE, but a smaller value permits faster detection of a permanent error condition. The default value for this parameter is 5.

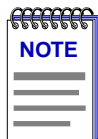
#### Inactivity Timer

This parameter is only relevant if **PAD Type** (see below) is HPAD. It is the amount of time (in seconds) that the FRX will wait with no activity on the port before it declares the port is down. The default value for this parameter is 50.

#### Physical Port Interface

The physical port interface is defined by the port's connector and cabling type, and must be configured as follows:

- For the FRX4000 and SmartSwitch 1800, port 0 and port 1 are always RS-232;



*If you have installed the optional CSU/DSU card on an FRX4000 or SmartSwitch 1800, it will logically take port 1, and you must configure certain CSU/DSU parameters through console management. Refer to your FRX or SmartSwitch 1800 hardware documentation for more information.*

- For the FRX4000, ports 2 and 3 are determined by the attached cables: RS-232, V.35, RS-449, or X.21;



- For the SmartSwitch 1800, ports 2 and 3 are determined by the attached cables: RS-232, V.35, or RS-449;
- For the FRX4000, ports 4-7 are determined by the expansion Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, and X.21. (RS-449 and X.21 interfaces require an RS-422 LIC.)
- For the FRX6000, ports 0-7 on each RLP are determined by the Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, RS-530 and X.21. (RS-449, RS-530, and X.21 interfaces require an RS-422 LIC.)

### **PAD Type**

The most common SNA networking requirement is for communication between an SNA host computer (PU type 4) and control units (PU type 2). This is accomplished via an HPAD (Host PAD) and TPAD (Terminal PAD). The host computer FEP (front end processor) is connected to the HPAD and the cluster controller is connected to a TPAD.

XPAD is used for networking of statistical multiplexers and other bit-sync devices.

The default value for this parameter is TPAD.

### **LPDA Support**

This field specifies the version, if any, of Link Problem Determination Aid that can be used by a host program (e.g., NetView or VTAM) or controller program (e.g., NCP) to test status and to control the line and remote interface. Select from two versions, lpda-1 or lpda-2; or select None, if no version will be used. The default value for this parameter is None.

### **NRZ Data Encoding**

This field determines the level of data encoding. If you select **Yes**, then NRZ (Non-Return to Zero) will be on. This means that 1 represents high-level encoding and 0 is low-level. If you select **No**, then NRZ is off, which means that 1 represents no change in level, and 0 is a change.

Always use NRZ for all SNA modes, unless there is a site-specific configuration that needs NRZI (Non-Return to Zero Inverted). In that case, select **No** because NRZ off means that NRZI is on.

### **Generate Clock**

This setting specifies whether the port will generate the clock, or timing, necessary to synchronize traffic over the link. If the port is a physical DCE (as determined by the port's I/O cable interface), specify **Yes**, since the physical DCE generates clock. If the port is a physical DTE, specify **No**. The default value for this parameter is **Yes**.

### Receive Clock from DTE

This parameter is relevant only if the **Physical Port Interface** (see above) is something other than RS-232 and **Generate Clock** is set to **Yes**. If this parameter is set to **Yes**, it allows the clock (timing) signal to be looped back from the DTE using the Terminal Timing (TT) signal, which can be helpful on high-speed lines. Generally, if the local interface is a physical DCE and the line speed is above 256 Kbps, this parameter should be set to **Yes**; however, make sure the DTE is configured to provide the terminal timing. The default value for this parameter is **No**.

### Disable Rqst Disconnect

This parameter is only relevant if the PAD type is HPAD. If this value is set to **Yes**, it prevents the HPAD from sending a Disconnect Request to the host if the HPAD-TPAD connection is broken. The default value for this parameter is **No**.

### Idle Fill Char

This field specifies a character that will be inserted into the stream when the SNA link is idle. The two choices are hex-ff and hex-7e; the default value is hex-ff.

### L1 Duplex

This field determines level-1 signal operation on RS-232 ports. If Full is selected, RTS (Request to Send), CTS, (Clear to Send) and DCD are always high (and are raised by the appropriate side).

If Half is selected:

- When the DTE is ready to transmit, it asserts RTS, waits for CTS to become high, then starts transmitting. When transmission is finished, the DTE drops RTS (and the DCE should drop CTS). DCD is low during this period.
- When the DCE is ready to transmit, it checks to see that RTS and CTS are not high, then it raises DCD and starts transmitting. When transmission is done, the DCE drops DCD. RTS and CTS are low during this period

For both Full and Half L1-Duplex, the DTE raises DTR (Data Terminal Ready) and the DCE raises DSR (Data Set Ready).

The default value for this parameter is Full.



*This parameter must be configured correctly, or the PU will not become active.*

### Changing Configuration Values

You can edit the values in any field; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.

If you have made changes to the fields but would like to revert back to the previous values, click on the **Refresh** button.

3. Click on  to save your changes.

### Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

### SDLC PU Configuration

After you have configured the SNA port, you must also define the physical units (PU) that will communicate via that SNA port. You can use the SDLC Physical Unit Subscriber Table to define PUs.

To access the window:

1. Click mouse button 3 on the SNA port of interest to display the Port menu.
2. Drag down to **SDLC PU Configuration**, and release. The SDLC Physical Unit Subscriber Table, [Figure 7-2](#), will appear.

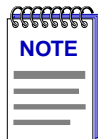
Address	Local Subscriber	Remote Subscriber	LPDA Id	LLC2	Auto Call	Retry Time	Retry Count	L2 Data Mode
1	09000301	0965030	0	Yes	Yes	60	0	Alternate
2	09000302	0965030	0	Yes	No	60	0	Alternate
3	09000303	09650303	0	Yes	No	60	0	Alternate
4	09000304	09650304	0	Yes	No	60	0	Alternate
5	09000305	09650305	0	Yes	No	60	0	Alternate
6	09000306	09650306	0	Yes	No	60	0	Alternate
7	09000307	09650307	0	Yes	No	60	0	Alternate

Address (00-ff hex) :       Auto Call Enabled :  Yes  
 Local Subscriber Id :       Retry Time (15-225 sec) :   
 Remote Subscriber Id :       Retry Count (0-255) :   
 LPDA Resource Id (0-255) :       L2 Data Mode :   
 LLC2 Connection :  Yes

Figure 7-2. SDLC Physical Unit Subscriber Table

The SDLC Physical Unit Subscriber Table allows you to configure the following parameters:



*An SNA TPAD subscriber can specify only one remote device, which can be an HPAD or an X.25 connection to the host. An HPAD subscriber can specify up to 16 remote devices, any of which can be a TPAD or an X.25 connection to the host. An XPAD subscriber can specify only one remote device, which must be another XPAD.*

### Address

This is the SDLC PU Station Address, 00 - ff, that identifies the PU you are configuring. It must match the ADDR parameter set in the macro PU in the VTAM configuration.

### Local Subscriber Id

This is the subscriber address of the local end of a SNA connection. Enter a Subscriber ID of up to 15 digits. This is the same subscriber ID that is specified in the Subscriber Table (see Chapter 4, Configuring the Subscriber Table, for Subscriber ID conventions). Each local subscriber configured here must also be configured in the Subscriber Table, so that routing information for each subscriber address can be specified.

### **Remote Subscriber Id**

This is the subscriber address of the remote end of a SNA connection. It is used by the local device to identify where a call is going. Enter a Subscriber ID of up to 15 digits. A Subscriber ID record must also be configured for this address (see Chapter 4, Configuring the Subscriber Table for Subscriber ID conventions).

If the PU is one end of a connection to a logical port in the FRX or SmartSwitch 1800, this ID must match a Subscriber ID configured for the logical port.

### **LPDA Resource Id**

LPDA requires both a PU name and an LU (logical unit) ID. This field identifies a LU on the PU. The Resource ID value must match the NetView LOCADDR. The default value for this parameter is 0.

### **LLC2 Connection**

This field specifies whether SDLC-LLC2 conversion will be done on the PU connection, either locally or at a remote node via a logical or physical port. If the PU will be used for SDLC-LLC2 conversion, this field must be set to **Yes**. The default value for this parameter is **No**.

### **Auto Call Enabled**

This parameter enables automatic calling between SNA ports when the controller (identified by Link Address) becomes active. If **Yes** is selected on an SNA port, an X.25 call will be made from the local port to the remote subscriber port.

The default value for this parameter is **No**. If you have configured the SNA port with a **PAD Type** of TPAD, you should set Autocall to **Yes**. If you have configured the SNA port with a **PAD Type** of HPAD, set Autocall to **No**.

### **Retry Time**

The amount of time (in seconds) between Auto Call retries (see above). If Auto Call is disabled, (if **No** was selected), this field will be grayed out. The default value for this parameter is 60.

### **Retry Count**

The maximum number of times an Auto Call (see above) will be sent. If Auto Call is disabled, (if **No** was selected), this field will be grayed out. The default value for this parameter is 0 (indefinite).

### **L2 Data Mode**

This field determines whether transmission will be in one or two directions at the same time. If you select Two Way Alternate it will be in one direction at a time; if you select Two Way Simultaneous, it will be in two directions at the same time. The default value for this parameter is Two Way Alternate.

### Changing SDLC PU Subscriber Values

To edit the values assigned to each SDLC PU Subscriber:

1. If you wish to modify an existing entry, be sure that entry is highlighted in the list box portion of the window.
2. Enter and/or edit the values displayed in the text boxes, as desired. (Remember, some values which are settable from this window must mirror values configured elsewhere; be sure these values match as necessary.)
3. Click on  to create a new entry, or on  to edit the entry currently selected in the list box.

### Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

### SDLC PU LLC2 Configuration

If SDLC-LLC2 conversion will be performed on the PU connection, you must configure the PU LLC2 parameters. You can use the SDLC LLC2 Configuration window to define PUs. (If the PU is not part of an SDLC-LLC2 connection, you do **not** have to configure these parameters.)

To access the window:

1. Click mouse button 3 on the SNA port of interest to display the Port menu.
2. Drag down to **SDLC PU LLC2 Configuration**, and release. The SDLC LLC2 Configuration window, [Figure 7-3](#), will appear.

SDLC LLC2 Configuration RLP 0 Port 3

Address	Local SAP	Local MAC	IDBLK	IDNUM	Ti	T1	T2	N2	N3	Tw	BAG	Priority	SuppressXID
1	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No
2	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No
3	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No
4	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No
5	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No
6	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No
7	4	00:00:00:00:00:00	0	0	30	10	100	8	3	7	0	0	No

Address (00-ff hex) :       T2-Recv Ack Timer (100-5000 ms) :   
 Local SAP Address (0-252) :       N2-Max LPDUs (0-255) :   
 Local MAC Address :       N3-Max Info LPDUs (1-127) :   
 IDBLK (0-4095) :       Tw-Max Out LPDUs (1-127) :   
 IDNUM (0-1048575) :       Bandwidth Allocation Group (0-16) :   
 Ti-Inactivity Timer (1-50 sec) :       Priority (0-9) :   
 T1-LLC2 Reply Timer (1-250 ms) :       Suppress XID :

Figure 7-3. SDLC LLC2 Configuration window

The SDLC LLC2 Configuration window allows you to configure the following parameters:

#### Address

This is the SDLC PU Station Address, 00 - ff, that identifies the PU you are configuring. It must match the ADDR parameter set in the macro PU in the VTAM configuration.

#### Local SAP Address

This is the remote service access point (SAP) address used to connect the PU to the host. This parameter is relevant only in a connection to a 3174 or AS/400-type setup where a specific source SAP address is required. If the LLC2 session will run over a native LLC2 frame relay interface, this parameter will be ignored.

#### Local MAC Address

This address identifies the PU to the host. Like the local SAP address, this parameter is relevant only in a connection to a 3174 or AS/400-type setup where a specific source MAC address is required. If the LLC2 session will run over a native LLC2 frame relay interface, this parameter will be ignored.

### **IDBLK**

This parameter is used in conjunction with the **IDNUM** parameter (see below) in generating the Node field in an XID (Exchange Identification) frame (format 0 or 3) to establish a link station connection to the host. If both IDBLK and IDNUM are set to 0, the Node field of the XID frame will be provided by the attached SDLC device. The node will send an XID command to the remote node to indicate that the SDLC device should be polled for an XID.

### **IDNUM**

This parameter is used in conjunction with the **IDBLK** parameter (see above) in generating the Node field in an XID frame (format 0 or 3) to establish a link station connection to the host. If both IDBLK and IDNUM are set to 0, the Node field of the XID frame will be provided by the attached SDLC device. The node will send an XID command to the remote node to indicate that the SDLC device should be polled for an XID.

### **Ti-Inactivity Timer**

This timer is used by the link station to detect an inoperative condition in either the remote link station or the transmission medium. The timer will be started if the T1-LLC2 Reply Timer has been reset (see below), if additional LLC protocol data units (LPDUs) have been sent by the remote link station, and if there are no outstanding acknowledgments or responses from the local link station.

If the local station does not receive an LPDU before the Ti-Inactivity Timer expires, the station must send an LPDU with the P bit set to B'1' to solicit the remote station's status. Recovery then proceeds as described under **T1-LLC2 Reply Timer**.

The value is the amount of time in seconds; the default value is 30.

### **T1-LLC2 Reply Timer**

The Reply Timer is used to detect the failure to receive a required acknowledgment or response from the remote link station. The link station will start the timer when it transmits either an Information LPDU or a Command LPDU with the P bit set to B'1'. (If the LPDU is sent while the timer is already running, the link station will reset the timer.)

The link station will reset the T1-LLC2 Reply Timer when it receives one of these:

- An REJ (Reject) LPDU, provided a Command LPDU with P bit set to B'1' is not outstanding;
- A Response LPDU with the F bit set to B'1';
- An Information or Supervisory LPDU with an  $N_R$  greater than the last  $N_R$  received and less than or equal to the line station's  $V_S$ , provided a Command LPDU with P bit set to B'1' is not outstanding.

If additional LPDUs are set from the remote link station after the local station has reset the T1 timer, the timer will be restarted if acknowledgments of, or responses to, those LPDUs are outstanding. If no acknowledgments/responses are outstanding, the link station will start the **Ti Inactivity Timer** (see above).



If the T1 Timer expires and acknowledgments or responses are still outstanding, the link station will send one of the following, then restart the T1 Timer:

- A Supervisory LPDU with the P bit set to B'1' to solicit remote link station status
- Any Unnumbered LPDUs that were not responded to the first time they were sent.

If acknowledgments or responses are still outstanding after the number of tries specified in the **N2-Max LPDUs** parameter (see below), the link station will declare the link inoperative.

The value specified for the T1 LLC2 Reply Timer should allow for any delays introduced by the MAC sublayer (e.g., queuing). The value is the amount of time in 100 millisecond units; the default value is 10.

#### **T2-Rcv Ack Timer**

This is the Receiver Acknowledgment Timer, used by the link station to delay sending an acknowledgment of a received Information LPDU. The timer is started when the LPDU is received, and reset when the acknowledgment is sent. If the timer expires before the acknowledgment is sent, it must be sent as soon as possible. The value is the amount of time in milliseconds; the default value is 100. The value must be less than the value for the **T1-LLC2 Reply Timer** (see above) to ensure that the remote link station will receive the delayed acknowledgment before the T1 Timer expires.

#### **N2-Max LPDUs**

This is the maximum number of times that an LPDU (including Information LPDUs resent after a checkpoint operation) will be sent following the expiration of the T1 Timer. The default value for this parameter is 8.

#### **N3-Max Info LPDUs**

This is the number of Information LPDUs that will be received by the local station before it sends an acknowledgment. This parameter is used in conjunction with the **T2-Rcv Ack Timer** to allow stations to reduce traffic. A counter is initialized to the value specified, and is decremented by one each time a valid sequential Information LPDU is received. When the counter reaches 0, an acknowledgment is sent. The counter is reset whenever an Information or Supervisory acknowledgment LPDU is sent by the local station. The default value for this parameter is 1.

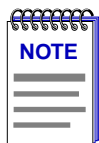
#### **Tw-Max Out LPDUs**

This is the maximum number of sequentially numbered Information LPDUs that the link station can have outstanding. The default value for this parameter is 1.

#### **Bandwidth Allocation Group**

This parameter assigns the LLC2 host to one of 16 Bandwidth Allocation Groups (BAG). The default value for this parameter is 0.

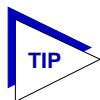
BAGs regulate bandwidth usage by outgoing traffic on the physical link and can ensure that response time-sensitive traffic gets access to the available frame relay bandwidth. Up to 16 groups can be configured through console management (refer to your FRX or SmartSwitch 1800 hardware documentation for more information).



*Bandwidth allocation groups cannot currently be configured via SPMA; for more information on configuring these groups, see your FRX or SmartSwitch 1800 hardware documentation.*

### Priority

This field prioritizes the interface for traffic within the device; the higher the number, the higher the priority. This priority has no effect on traffic exiting the device. Priorities are configured on all logical interfaces that use a physical frame relay port. The FRX or SmartSwitch 1800 processor uses these priorities to help determine the order in which it will process protocols. The default value for this parameter is 0.



*When configuring priorities, be sure to consider the types of traffic being routed on other connections in the node.*

### Suppress XID

If **Yes** is selected, this parameter prevents the FRX or SmartSwitch 1800 from returning an XID (Exchange Identification) in response to a null XID. This might be desirable if the remote TPAD is not running PU 2.1. It should be noted that even if an XID is sent, an SNRM (Set Normal Response Mode) immediately follows, so the connection will be established. The default value for this parameter is **No**.

## Changing SDLC PU LLC2 Values

To edit the SDLC PU LLC2 values:

1. If you wish to modify an existing entry, be sure that entry is highlighted in the list box portion of the window.
2. Enter and/or edit the values displayed in the text boxes, as desired. (Remember, some values which are settable from this window must mirror values configured elsewhere; be sure these values match as necessary.)
3. Click on **Add** to create a new entry, or on **Modify** to edit the entry currently selected in the list box.

## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## SDLC Link Station Configuration

You can use the SDLC Link Station Configuration window to configure SDLC link station entries.

To access the window:

1. Click mouse button 3 on the SNA port of interest to display the Port menu.
2. Drag down to **SDLC LS Entries**, and release. The SDLC Link Station Configuration window, [Figure 7-4](#), will appear.

SDLC Link Station Configuration RLP 0 Port 3

Address	Name	Desired Op. State
1	h0301	Active
2	H0302	Active
3	h0303	Active
4	h0304	Active
5	h0305	Active

Address (00-ff hex) :  RNR Limit :

Name :  Group Poll Address (0-254) :

Max Rx PDU Size :  Desired Operational State :

Max Tx PDU Size :  Desired State At Startup :

Reply Timeout :  Modulus :

Max Rx UnACK I-Frames (1-127) :  Data Mode :

Max Tx UnACK I-Frames (1-127) :  Support SIM, RIM Frames :

Retries In Sequence (0-128) :  Transmit-Receive Capabilities :

Retry Sequence Interval :

Retry Sequence Repeat Count :

Add Modify Delete

Refresh Close

Figure 7-4. SDLC Link Station Configuration window

The SDLC Link Station Configuration window allows you to configure the following parameters:

**Address**

This is the SDLC PU Station Address, 00 - ff, that identifies the PU you are configuring. It must match the ADDR parameter set in the macro PU in the VTAM configuration.

**Name**

Enter the name of the local SDLC link station.

**Max RX PDU Size**

This is the maximum PDU size that the local link station can receive from the adjacent link station. This value is sent in the XID to the ALS and includes the Transmission Header (TH) and the Request Header (RH).

**Max TX PDU Size**

This is the maximum PDU size the local link station can send to the adjacent link station before having received any XID from the ALS. This value includes the Transmission Header (TH) and the Request Header (RH).

**Reply Timeout**

This field specifies a reply timeout (in 1/100ths of a second) for an SDLC link station. If the link station does not receive a response to a poll or message before the specified time expires, the appropriate error recovery will be initiated. The default value for this parameter is 100.

**Max Rx UnACK I-Frames**

This field specifies the maximum number of unacknowledged I-frames an SDLC link station may receive. The default value for this parameter is 7.

**Max Tx UnACK I-Frames**

This field specifies the maximum number of consecutive I-frames an SDLC link station may send without an acknowledgment. The default value for this parameter is 1.

**Retries in Sequence**

This is the number of retries in a retry sequence for the local SDLC link station. A retry sequence is a series of retransmitted frames (data or control) for which no positive acknowledgment is received. The default value for this parameter is 15.

**Retry Sequence Interval**

This is the interval (in 1/100ths of a second) between retry sequences for the local SDLC link station if multiple retry sequences are specified. The default value for this parameter is 0.

**Retry Sequence Repeat Count**

This field specifies the number of times a retry sequence will be repeated for the local SDLC link station. The default value for this parameter is 0.

**RNR Limit**

This specifies the length of time (in 1/100ths of a second) an SDLC link station will allow its adjacent link station to remain in a busy (RNR) state before declaring it inoperative. A value of 0 means there is no limit. The default value for this parameter is 18000.

**Group Poll Address**

This field defines the group poll address for this link station. If group poll is not in effect for this link station, the value should be 0.

**Desired Operational State**

This is the desired state of the SDLC station, Active or Inactive. The default value for this parameter is Active.

**Desired State at Startup**

This is the desired state at startup of the SDLC station, Active or Inactive. The default value for this parameter is Active.

**Modulus**

This parameter specifies the modulus for the SDLC link station. The modulus determines the size of the rotating acknowledgment window used by the SDLC link station pair. The default value for this parameter is 8.

**Data Mode**

Use this field to specify whether communications mode with the adjacent link station is Half (two-way alternate) or Full (two-way simultaneous). The default value for this parameter is Half.

**Support SIM, RIM Frames**

This parameter determines whether the link station supports transmission and receipt of Set Initialization Mode (SIM) and Request Initialization Mode (RIM) control frames. The default value for this parameter is **No**.

**Transmit-Receive Capabilities**

This parameter controls the transmit-receive capabilities for this link station, two-way alternating (twa) or two-way simultaneous (tws). The selected value establishes the value of the transmit-receive capability indicator sent in the XID image to the adjacent link station.

## Changing SDLC Link Station Values

To edit the SDLC Link Station values:

1. If you wish to modify an existing entry, be sure that entry is highlighted in the list box portion of the window.
2. Enter and/or edit the values displayed in the text boxes, as desired. (Remember, some values which are settable from this window must mirror values configured elsewhere; be sure these values match as necessary.)
3. Click on  to create a new entry, or on  to edit the entry currently selected in the list box.

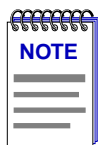
## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## Configuring LLC2

LLC2 support in the FRX and SmartSwitch 1800 provides a local or remote connection over frame relay (via RFC 1490) or X.25 (via QLLC) between two SNA devices, one attached to a LAN and the other attached to either another LAN or a frame relay-compliant SNA / APPN (Advanced Peer-to-Peer Networking) device. Each SNA host and terminal accessing the FRX or SmartSwitch 1800, via SDLC, LLC2, frame relay, or X.25, will appear to a local LLC2-attached terminal or host as if it is directly connected to the local LAN.



*If LLC2 is being used, Bridging must also be loaded and configured. You must configure a Virtual LAN ID to identify a virtual bridge that connects the LLC2 function to LAN interfaces. See Chapter 11, Bridge Configuration, for information on setting the Virtual LAN ID and other bridging parameters.*

You must configure each SNA/LLC2 host device that will connect to an FRX or SmartSwitch 1800 running LLC2. You can configure a host using the SNA/LLC2 Host Table.

To access the table:

1. Click on the  button to display the Device menu.

2. Drag down to **SNA/LLC2 Hosts Table**, and release. The SNA/LLC2 Host Table, [Figure 7-5](#), will appear.

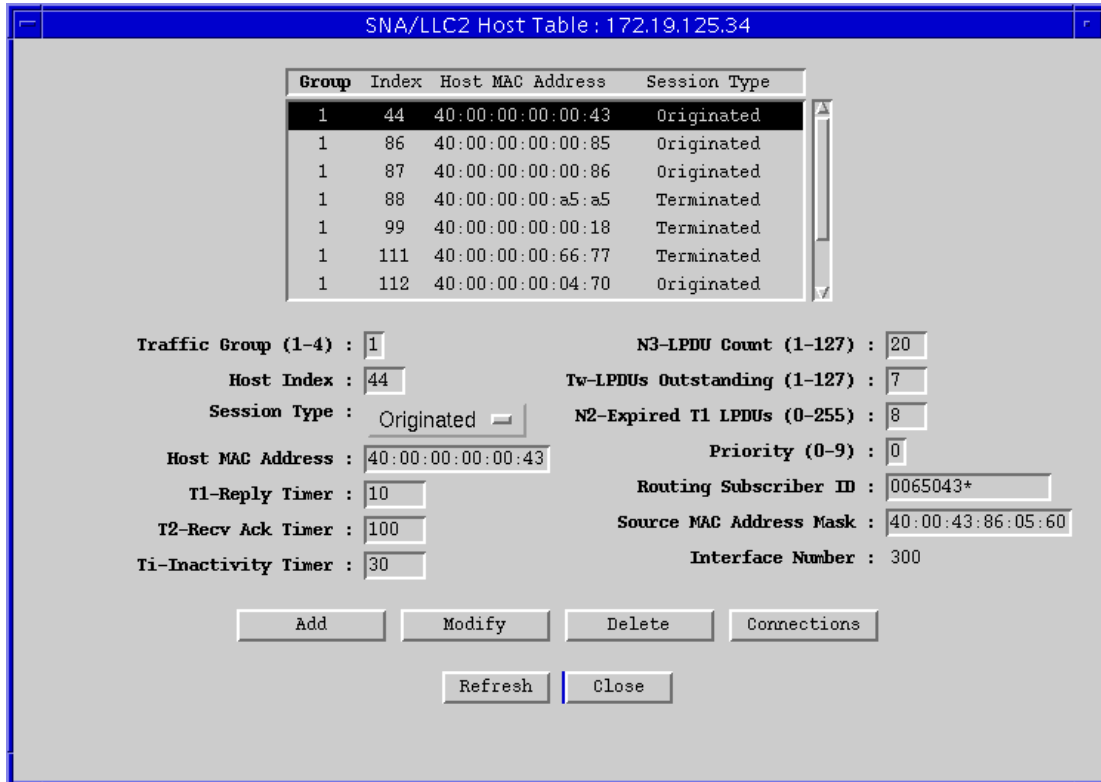


Figure 7-5. The SNA/LLC2 Host Table

The list box at the top of the window displays the LLC2 hosts that have already been configured. It lists the hosts' MAC addresses and identifies each LLC2 session as Originated or Terminated. In an Originated session, the host initiates LLC2 sessions; in a Terminated session, the host accepts sessions destined for the address. A host-to-terminal connection is always initiated by the terminal.

The fields and buttons in the lower portion of the window allow you to add new entries, and modify or delete existing ones.

The SNA/LLC2 Host Table allows you to configure the following parameters:

#### Traffic Group

This is the traffic group associated with the LLC2 interface. It is always set to 1.

#### Host Index

This is the host number 0 - 128. The default value is 0.

**Session Type**

If you select Originated, the FRX or SmartSwitch 1800 will initiate LLC2 sessions from the configured Host MAC Address. If Terminated, the node will accept LLC2 sessions destined for the configured Host MAC Address. A host address can be configured for one Originated and one Terminated session, but no more than one each. The default value for this parameter is Terminated.

**Host MAC Address**

This is the MAC address of the host or workstation to which an SNA/LLC2 device needs to connect.

If the remote host will be attached via an Ethernet interface in the FRX or SmartSwitch 1800 and the remote device is attached via a Token Ring, (or vice versa), this MAC address will be “bit-swapped” internally, because of the differences in frame formatting between Ethernet and Token Ring. In this case, the address must be “bit-swapped” again, so the remote device will receive an address in the correct format.

Bit swapping is done by reversing the order of the bits (digits) within each byte (pair of digits) of the hexadecimal address, while leaving the sequence of the bytes unchanged.

For example, to bit-swap the hex address 400010001088:

1. Break the address into pairs of digits: | 40 | 00 | 10 | 00 | 10 | 88 |
2. Reverse the digits within each pair: | 04 | 00 | 01 | 00 | 01 | 88 |
3. Replace each digit as specified in the following list. This reverses the binary bits of each digit. For example, 7 (0111 binary) becomes E (1110 binary).

Digit	Convert to	Digit	Convert to	Digit	Convert to
0	0	6	6	C	3
1	8	7	E	D	B
2	4	8	1	E	7
3	C	9	9	F	F
4	2	A	5		
5	A	B	D		

Using this example, | 04 | 00 | 01 | 00 | 01 | 88 |  
 converts to: | 02 | 00 | 08 | 00 | 08 | 11 |

4. Enter the bit swapped value (e.g., 020008000811) as the Host MAC Address. This value will arrive at the host as the proper address (e.g., 400010001088) after being translated.



**T1-Reply Timer**

The Reply Timer is used to by the local node to detect a failure by the remote station to send a required acknowledgment or response. The local node will start the timer when it transmits either an Information LPDU or a Command LPDU with the P bit set to B'1'. (If the LPDU is sent while the timer is already running, the local node will reset the timer.)

The local node will reset the T1-Reply Timer when it receives one of these:

- An REJ (Reject) LPDU, provided a Command LPDU with P bit set to B'1' is not outstanding;
- A Response LPDU with the F bit set to B'1';
- An Information or Supervisory LPDU with an  $N_R$  greater than the last  $N_R$  received and less than or equal to the line station's  $V_S$ , provided a Command LPDU with the P bit set to B'1' is not outstanding.

If additional LPDUs are set from the remote station after the local node has reset the T1 timer, the timer will be restarted if acknowledgments of or responses to those LPDUs are outstanding. If no acknowledgments/responses are outstanding, the local node will start the **Ti-Inactivity Timer** (see below).

If the T1 Timer expires and acknowledgments or responses are still outstanding, the local node will send one of the following, then restart the T1 Timer:

- A Supervisory LPDU with the P bit set to B'1' to solicit remote link station status;
- Any Unnumbered LPDUs that were not responded to the first time they were sent.

If acknowledgments or responses are still outstanding after the number of tries specified in the **N2-Expired T1 LPDUs** parameter (see below), the local node will declare the link inoperative.

The value specified for the T1-Reply Timer should allow for any delays introduced by the MAC sublayer (e.g., queuing). The value is the amount of time in 100 millisecond units; the default value is 10.

**T2-Recv Ack Timer**

This is the Receiver Acknowledgment Timer, used by the local node to delay sending an acknowledgment of a received Information LPDU. Delaying acknowledgments for as long as possible minimizes the number of acknowledgments that must be sent (since more than one received frame can be acknowledged with one transmission).

The timer is started when the LPDU is received, and reset when the acknowledgment is sent. If the timer expires before the acknowledgment is sent, it must be sent as soon as possible.

The value is the amount of time in milliseconds; the default value is 100. The value must be less than the value for the **T1-Reply Timer** (see above) to ensure that the remote link station will receive the delayed acknowledgment before the T1 Timer expires.

#### **Ti-Inactivity Timer**

This timer is used by the local node to detect an inoperative condition in either the remote link station or the transmission medium. The timer will be started if the T1-Reply Timer has been reset (see above), and additional LPDUs have been sent by the remote link station, and there are no outstanding acknowledgments or responses from the local node.

If the local node does not receive an LPDU before the Ti-Inactivity Timer expires, the station must send an LPDU with the P bit set to B'1' to solicit the remote station's status. Recovery then proceeds as described under **T1-Reply Timer** (see above).

The value is the amount of time in seconds; the default value is 30.

#### **N3-LPDU Count**

This is the number of Information LPDUs that will be received by the local node before it sends an acknowledgment. This parameter is used in conjunction with the **T2-Recv Ack Timer** to allow stations to reduce traffic. A counter is initialized to the value specified, and is decremented by one each time a valid sequential Information LPDU is received. When the counter reaches 0, an acknowledgment is sent. The counter is reset whenever an Information or Supervisory acknowledgment LPDU is sent by the local node. The default value for this parameter is 3.

#### **Tw-LPDUs Outstanding**

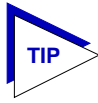
This is the maximum number of sequentially numbered Information LPDUs that the local node can have outstanding. When the number is reached, an acknowledgment will be sent. The default value for this parameter is 7.

#### **N2-Expired T1 LPDUs**

This is the maximum number of times that an LPDU (including Information LPDUs resent after a checkpoint operation) will be sent following the expiration of the T1 Timer. The default value for this parameter is 8.

#### **Priority**

This field prioritizes the interface for traffic within the device; the higher the number, the higher the priority. This priority has no effect on traffic exiting the device. Priorities are configured on all logical interfaces that use a physical frame relay port. The FRX or SmartSwitch 1800 processor uses these priorities to help determine the order in which it will process protocols. The default value for this parameter is 0.



When configuring priorities, be sure to consider the types of traffic being routed on other connections in the node.

### Routing Subscriber ID

This field associates a Subscriber ID with the LLC2 host. Enter a number up to 15 digits. An asterisk wildcard can be used as a final digit (but the ? wildcard is not valid). If fewer than 15 digits are entered, an asterisk must be the final character.

The Routing Subscriber ID partially defines the Local Subscriber ID in the Connections Table defined for each LLC2 host (see [Configuring LLC2 Host Connections, page 7-24](#)).

### Source MAC Address Mask

This parameter is used to identify the FRX and SmartSwitch 1800 to inbound frames from a local LAN in an Originated LLC2 session. (If you have selected Terminated as your **Session Type**, this field will be grayed out.)

Source address masks and host MAC addresses are placed in a forwarding list that is checked by the firmware when a frame is received. If the MAC address in an incoming frame matches a configured Source MAC Address Mask, the frame will be passed through the node for transmission out the frame relay interface.

Enter an address up to eight hexadecimal digits. The first digit must be 4, 5, 6, or 7, and an asterisk wildcard can be used as a final digit. If fewer than eight actual digits (not including an asterisk) are specified, zeros will be added to total eight actual digits. This value must not conflict with the Locally Administered MAC Address described in your FRX and SmartSwitch 1800 hardware documentation.

### Interface Number

This read-only field defines the LLC2 interface number associated with this host entry and will always be 300.

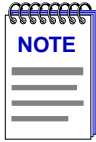
## Changing Configuration Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.

If you have made changes to the fields but would like to revert back to the previous values, click on the **Refresh** button.

3. Click on  to save your changes.



After you have made system-level changes (such as configuring LLC2), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.

## Configuring LLC2 Host Connections

You can configure the connections for each LLC2 Host by using the Originated or Terminated Connections Table. To access the Connections Table:

1. In the SNA/LLC2 Host Table, highlight the host whose connections you wish to configure.
2. Click on the **Connections** button at the bottom of the SNA/LLC2 Host Table window. This will bring up the Connections Table for the host that was highlighted. If the Session Type of that host was Originated, then the Originated Connections Table will appear. If the Session Type of that host was Terminated, then the Terminated Connections Table will appear.

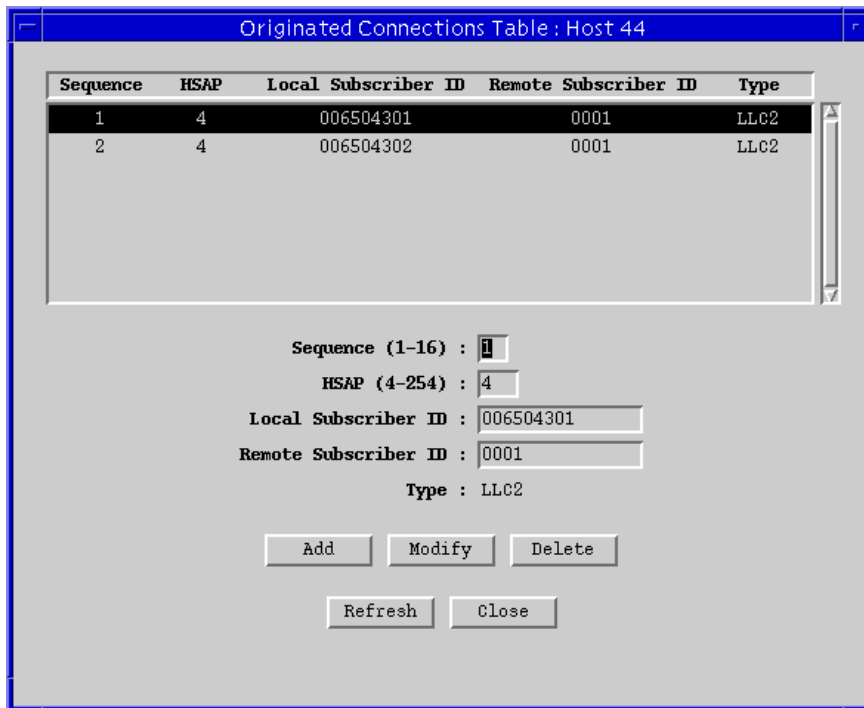


Figure 7-6. Originated Connections Table

The list box at the top of the window displays any connections that have already been configured. The fields and buttons in the lower portion of the window allow you to add new entries, and modify or delete existing ones.

The Connections Table allows you to configure the following parameters:

**Sequence**

This is simply a sequence number to allow selection of a line in the display.

**HSAP**

This is the host service access point (HSAP) address used to connect to the host. This must match the SSAP (source SAP) in a frame received from the local LAN or the DSAP (destination SAP) in a frame from the remote link station.

**Local Subscriber ID**

This is the subscriber address assigned to the local end of the SNA connection. If you are configuring an LLC2-to-SDLC link, this address must match the **Remote Subscriber ID** parameter configured in the SDLC Physical Unit Subscriber Table (see [SDLC PU Configuration, page 7-7](#)). If you are configuring an LLC2-to-LLC2 connection, this address must match the **Remote Subscriber ID** in the remote nodes's Connections Table.

The Local Subscriber ID can be up to 15 digits long, and must begin with all of the actual Routing Subscriber ID configured in the SNA/LLC2 Host Table. The Local Subscriber ID can contain an asterisk as the final digit; if so, the asterisk will not be a "universal" wildcard, but instead will include the range 000-511, or 00-99 if 13 digits precede the wildcard, or 0-9 if 14 digits precede the wildcard.

**Remote Subscriber ID**

This is the subscriber address assigned to the remote end of the SNA connection. If you are configuring an LLC2-to-SDLC link, this address must match the **Local Subscriber ID** parameter configured in the SDLC Physical Unit Subscriber Table (see [SDLC PU Configuration, page 7-7](#)). If you are configuring an LLC2-to-LLC2 connection, this address must match the **Local Subscriber ID** in the remote nodes's Connections Table.

The Remote Subscriber ID can be up to 15 digits long. It can contain an asterisk as the final digit; if so, the asterisk will not be a "universal" wildcard, but instead will include the range 000-511, or 00-99 if 13 digits precede the wildcard, or 0-9 if 14 digits precede the wildcard.

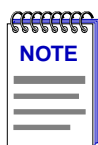
**Type**

This read-only parameter is relevant only in an Originated Connections Table, and is always LLC2.

## Changing Host Connections

To edit the Host Connection values:

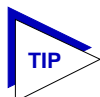
1. If you wish to modify an existing entry, be sure that entry is highlighted in the list box portion of the window.
2. Enter and/or edit the values displayed in the text boxes, as desired. (Remember, some values which are settable from this window must mirror values configured elsewhere; be sure these values match as necessary.)
3. Click on  to create a new entry, or on  to edit the entry currently selected in the list box.



*After you have made system-level changes (such as configuring LLC2), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Viewing SDLC Status

Four additional port-level menu selections provide statistical information regarding SDLC traffic and performance on a selected SNA port.



*The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.*

## SDLC Port Statistics

The SDLC Port Statistics window provides general information about the type of management traffic that is being transmitted across the selected port. To access the window:

1. Click mouse button 3 on the SNA port of interest to display the Port Menu.
2. Drag down to **SDLC Port Statistics**, and release. The SDLC Port Statistics window, [Figure 7-7](#), will appear.

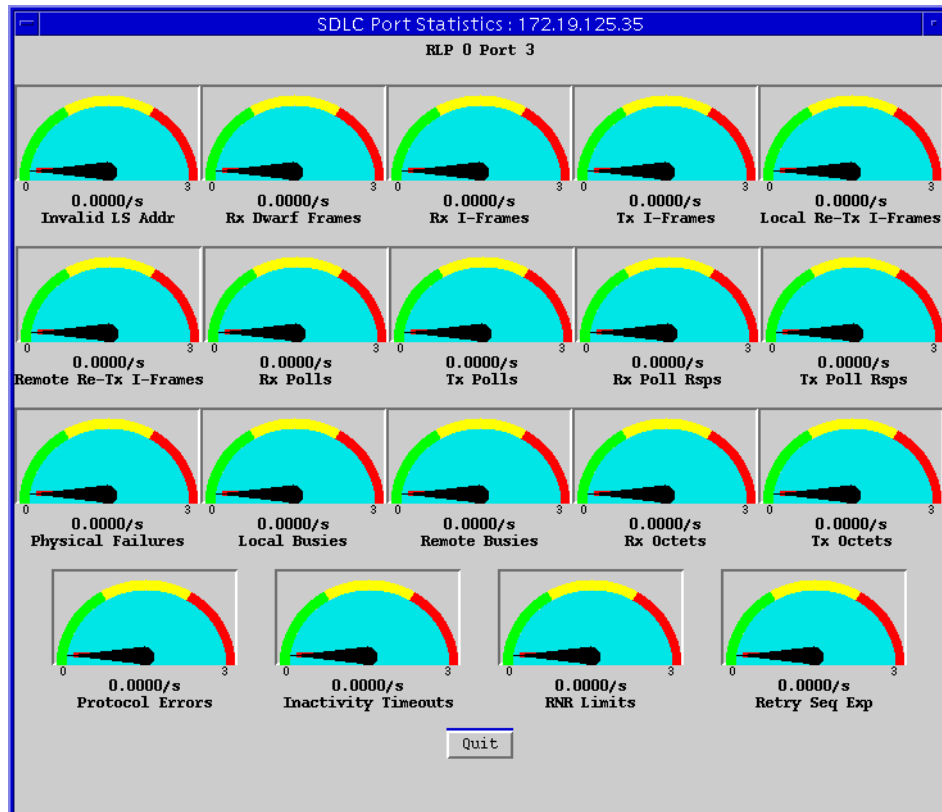


Figure 7-7. SDLC Port Statistics

The SDLC Port Statistics window provides the following statistical data:

#### Invalid LS Addr

The number of frames received by this port with invalid link station (LS) addresses, expressed as a rate (frames/second).

#### Dwarf Frames (Received)

The number of frames received by this port which were delivered intact by the physical layer, but were too short to be legal. A frame is considered to be too short if it is less than two bytes for a Modulus of 8, or less than three bytes for a Modulus of 128 (not counting the frame check sequence (FCS)). The number is expressed as a rate (frames/second).

#### I-Frames (Received and Transmitted)

The number of I-frames received or transmitted by the SDLC link stations on this port, expressed as a rate (frames/second).

**Local Re-Tx I-Frames**

The number of I-frames retransmitted by all local SDLC link stations on this port, expressed as a rate (frames/second).

**Remote Re-Tx I-Frames**

The number of I-frames retransmitted by remote link stations for all SDLC link stations on this port, expressed as a rate (frames/second).

**Polls (Received and Transmitted)**

The number of polls received or sent by this port since the port was created, expressed as a rate (polls/second).

**Poll Responses (Received and Transmitted)**

The number of poll responses received or sent by this port since the port was created, expressed as a rate (poll responses/second).

**Physical Failures**

The number of times this port has failed due to its physical media since port startup, expressed as a rate (failures/second).

**Busies (Local and Remote)**

The number of times the local or adjacent (remote) SDLC link stations on this port have entered a busy (RNR) state, expressed as a rate (busies/second).

**Octets (Received and Transmitted)**

The total octets received from or transmitted to adjacent SDLC link stations on this port, expressed as a rate (octets/second). This number covers the address, control, and information field of I-frames only.

**Protocol Errors**

The number of times the SDLC link stations on this port have deactivated the link as a result of having received a protocol violation from the adjacent link station, expressed as a rate (deactivations/second).

**Inactivity Timeouts**

The number of times the SDLC link stations on this port have deactivated the link as a result of no activity on the link, expressed as a rate (deactivations/second).

**RNR Limits**

The number of times the SDLC link stations on this port have deactivated the link as a result of their RNR (busy) Limit Timer expiring, expressed as a rate (deactivations/second).

**Retry Sequence Exp**

The number of times the SDLC link stations on this port have deactivated the link as a result of a retry sequence being exhausted, expressed as a rate (deactivations/second).



## SDLC Link Station General Statistics

The SDLC Link Station General Statistics window provides general information about the link station traffic that is being transmitted across the selected port. To access the window:

1. Click mouse button 3 on the SNA port of interest to display the Port Menu.
2. Drag down to **SDLC LS General Stats**, and release. The SDLC Link Station General Statistics window, [Figure 7-8](#), will appear.

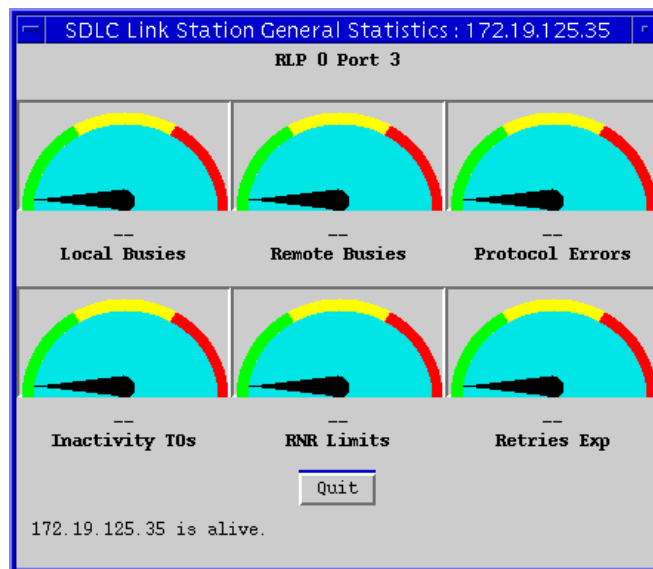


Figure 7-8. SDLC Link Station General Statistics

The SDLC Link Station General Statistics window provides the following statistical data:

### Busies (Local and Remote)

The total number of times that the local, or an adjacent (remote), SDLC link station has entered a busy (RNR) state since link station startup, expressed as a rate (busies/second).

### Protocol Errors

The number of times, since link station startup, when this SDLC link station has deactivated the link as a result of receiving a frame from its adjacent link station which was in violation of the protocol, expressed as a rate (deactivations/second).

### Inactivity T0s

The number of times, since link station startup, when this SDLC link station has deactivated the link as a result of no activity on the link, expressed as a rate (deactivations/second).

### RNR Limits

The number of times, since link station startup, when this SDLC link station has deactivated the link as a result of its RNR Limit Timer expiring, expressed as a rate (deactivations/second).

### Retries Exp

The number of times, since link station startup, when this SDLC link station has deactivated the link as a result of a retry sequence being exhausted, expressed as a rate (deactivations/second).

## SDLC Link Station Rx and Tx Statistics

The SDLC Link Station Rx and Tx Statistics windows provides information about the link station traffic that is being received and transmitted across the selected port. To access the windows:

1. Click mouse button 3 on the SNA port of interest to display the Port Menu.
2. Drag down to **SDLC LS Rx Stats** or **SDLC LS Tx Stats**, and release. The SDLC Link Station Rx or Tx Statistics window will appear. The SDLC Link Station Rx Statistics window is shown in [Figure 7-9](#).

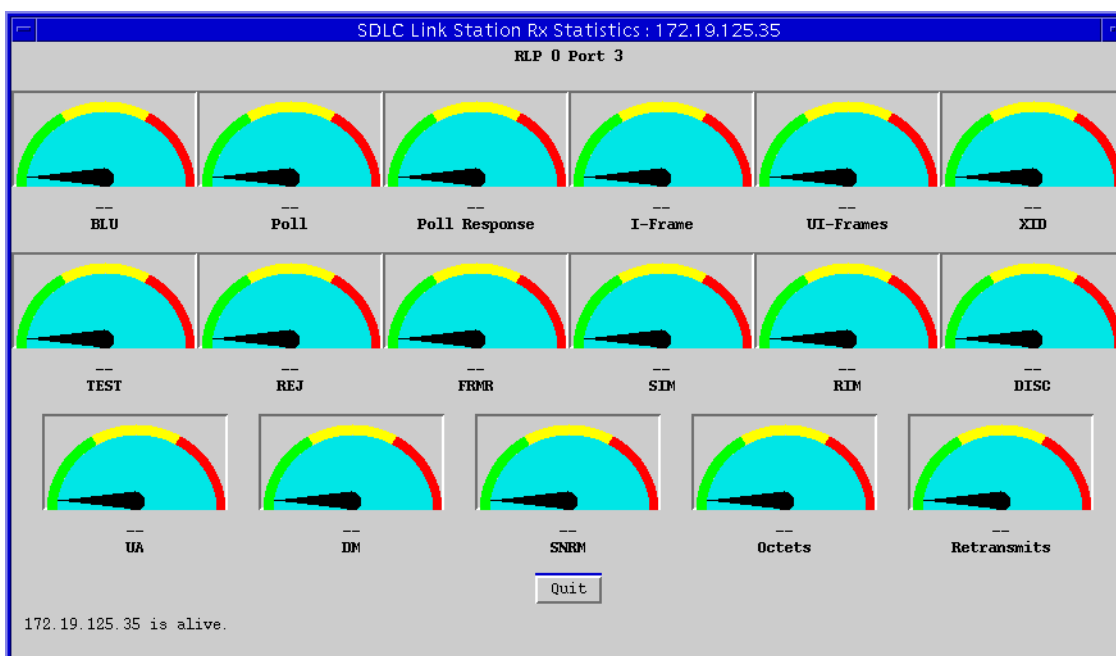


Figure 7-9. SDLC Link Station Rx Statistics

The SDLC Link Station Rx and Tx Statistics window provides the following statistical data:

**BLU**

The total Basic Link Units (BLU) received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (BLUs/second).

**Poll**

The total number of polls received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (polls/second).

**Poll Response**

The total number of poll responses received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (poll responses/second). This value includes I-frames that are received or sent in response to a poll.

**I-Frame**

The total number of I-frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (I-frames/second).

**UI-Frames**

The total number of UI-frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (UI-frames/second).

**XID**

The total number of XID frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (XID frames/second).

**TEST**

The total number of TEST frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (TEST frames/second).

**REJ**

The total number of REJ frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (REJ frames/second).

**FRMR**

The total number of Frame Reject (FRMR) Frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (FRMR frames/second).

**SIM**

The total number of Set Initialization Mode (SIM) frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (SIM frames/second).

**RIM**

The total number of Request Initialization Mode (RIM) frames received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (RIM frames/second).

**DISC**

The total number of Disconnect (DISC) requests received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (DISCs/second).

**UA**

The total number of Unnumbered Acknowledgment (UA) requests received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (requests/second).

**DM**

The total number of Disconnect Mode (DM) requests received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (requests/second).

**SNRM**

The total number of Set Normal Response Mode (SNRM/SNRME) requests received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (requests/second).

**Octets**

The total octets received from or transmitted to an adjacent SDLC link station since link station startup, expressed as a rate (octets/second). This includes the address, control, and information field of I-frames only.

**Retransmits**

In the Rx Statistics window, this is the total number of I-frames retransmitted by the remote link station because the N(s) received from that link station indicated that one or more I-frames sent by or to that station were lost.

In the Tx Statistics window, this is the total number of I-frames retransmitted to a remote link station because the N(r) received from that link station indicated that one or more I-frames sent by or to that station were lost.

This event causes the first missing I-frame of a window and all the subsequent I-frames to be retransmitted. This value is expressed as a rate (retransmits/second).

# BSC Interactive Configuration

*Configuring BSC Interactive ports; BSCI Subscriber Information; configuring devices connected to BSCI ports*

---

FRX4000, FRX6000, and SmartSwitch 1800 devices support binary synchronous communications (BSC) Interactive ports, used to connect IBM 3270 hosts to remote control units (CU) over frame relay or X.25.

For each physical port configured to run BSC Interactive (BSCI), three configuration windows are provided:

- The **BSCI Port Configuration** window allows you to configure basic parameters related to BSCI port operation;
- The **BSCI Subscriber Information** window provides information on local and remote subscribers for each BSCI port;
- The **BSCI Device Information** window lets you define the devices connected to the BSCI ports.

These windows and their functions are described in the following sections.

## Configuring BSCI Ports

Using the BSCI Port Configuration window, you can configure basic operating parameters for each of your BSCI ports.

To access the window:

1. Click mouse button 3 on the BSCI port of interest to display the Port Menu.
2. Drag down to **BSCI Port Configuration**, and release. The BSCI Port Configuration window, [Figure 8-1](#), will appear.

The screenshot shows a configuration window titled "BSCI Configuration RLP 0 Port 2". It contains the following parameters and their values:

Max Frame Size (21-4105) :	4105	Use EBCDIC :	Yes
Line Speed :	9600	Call Info in Request Packet :	Yes
Retransmission Period (1-9999) :	2000	Transparent Text Supported :	Yes
Max Retransmissions (1-99) :	5	End-to-End ACK :	No
Start Sync Chars (2-10) :	2	Full Duplex :	Yes
Trailing Pad Chars (1-10) :	1	Physical Port Interface :	RS-232
Poll Interval (100-1000 msec) :	500	Blocked Flag :	Disabled
No Response Timer (2-10 sec) :	2	Generate Clock :	Yes
No Response Retries (1-255) :	5	Receive Clock From DTE :	No
Error Retransmit Count (1-255) :	5	Clear VC on Last Dev Down :	No
NAK Retry Count (1-255) :	5	PAD Type :	tpad
Multidrop :	Yes	Answer Non Configured :	No
Slow Poll Retry Count (10-150) :	20	Connection Without Poll :	No
Slow Poll Retry Freq (1-200) :	20		

At the bottom of the window are two buttons: "Apply" and "Close".

Figure 8-1. BSCI Port Configuration

The BSCI Port Configuration window allows you to configure the following parameters:

**Max Frame Size**

Use this field to specify the maximum frame size that will be allowed to pass through this BSCI port. The default value for this parameter is 4105.

**Line Speed**

This field specifies the data transmission rate in bits per second. If this port is a physical DTE, specify the line speed that matches the speed of the device connected directly to the port. If the port is a physical DCE (i.e., the attached I/O cable is DCE) specify the clock speed of the serial port you are configuring. Valid values for this parameter are: 75, 150, 300, 600, 1200, 2400, 4800, 9600, 14400, and 19200. The default value for this parameter is 9600.

**Retransmission Period**

This is the length of time (in milliseconds) before the FRX or SmartSwitch 1800 will retransmit a data frame if the previous transmission of that data frame was not acknowledged. If the time expires, the timer will be reset, the data frame will be retransmitted, and the **Max Retransmissions** counter (see below) will be incremented.

The default value of 2000 milliseconds allows avoidance of unnecessary retransmission of frames that have merely been delayed.

**Max Retransmissions**

This is the maximum number of times the FRX or SmartSwitch 1800 will attempt to retransmit a data frame after the **Retransmission Period** (see above) expires. A larger value for this parameter increases the probability of an eventual successful transmission, but a smaller value permits faster detection of a permanent error condition. The default value for this parameter is 5.

**Start Sync Chars**

This is the number of synchronization characters that will be added to the beginning of each frame. The default value for this parameter is 2.

**Trailing Pad Chars**

This is the number of padding characters that will be appended to each frame. This ensures that the last significant character is sent before the data transmitter switches off. The default value for this parameter is 1.

**Poll Interval**

The amount of time (in milliseconds) between passes through the polling list. The default value for this parameter is 500.

**No Response Timer**

This timer begins after the FRX or SmartSwitch 1800 transmits a general poll or a data frame. It is the amount of time (in seconds) before the FRX or SmartSwitch 1800 transmits an NAK-EOT-General Poll sequence and increments the **No Response Retries** count (see below). The timer will stop upon receipt of any valid frame from the line. The default value for this parameter is 2.

**No Response Retries**

If a device is not responding to a poll, this count specifies how many times the device will be polled before the general poll sequence bypasses the device and moves on to the next one. The default value for this parameter is 5.

#### **Error Retransmit Count**

This field specifies the number of times the FRX or SmartSwitch 1800 will resend a block of data after the receiving device has detected an error in the block. The default value for this parameter is 5.

#### **NAK Retry Count**

This count specifies the number of times the FRX or SmartSwitch 1800 will send a frame when the receiving device is returning a NAK (negative acknowledgment).

#### **Multidrop**

If this parameter is set to **Yes**, the transmission will be multidrop (where there are several stations between end points); if **No**, the transmission will be point-to-point. The default value for this parameter is **No**.

#### **Slow Poll Retry Count**

This field is configurable only for ports configured for multidrop (see **Multidrop** parameter above). It specifies how many times a control unit (CU) that is not responding will be polled before it is put on the *slow poll list*. CUs on the *slow poll list* are polled with a frequency determined by the **Slow Poll Retry Frequency** parameter (see below). The default value for this parameter is 20.

#### **Slow Poll Retry Freq**

This field is configurable only for ports configured for multidrop (see **Multidrop** parameter above), and determines the frequency that control units (CU) on the *slow poll list* are polled. It specifies the number of times active CUs will be polled between pollings of the CUs on the *slow poll list* (see **Slow Poll Retry Count**, above). The higher the number, the more times active CUs will be polled, and the less frequently CUs on the *slow poll list* will be polled. The default value for this parameter is 20.

#### **Use EBCDIC**

This read-only parameter indicates that all devices on a line will use the EBCDIC character set for session polls. Because the FRX and SmartSwitch 1800 only support the EBCDIC character set, this value is always set to **Yes**.

#### **Call Info in Request Packet**

This read-only parameter is set to **Yes**, and indicates that call information will be included in a call request packet.

#### **Transparent Text Supported**

This read-only parameter is set to **Yes**, and indicates that all transmitted characters, including control character sequences, will be treated as data.

This parameter is useful for transmitting binary data and machine language computer programs without special coding. Data-link control character sequences transmitted this way must be preceded by a Data Link Escape (DLE) character (a value of 10 in hex) in order to be recognized as control characters.



**End-to-End ACK**

This read-only parameter is set to **No**, and indicates that management of acknowledgments will be handled locally at each end, rather than end-to-end across the network.

**Full Duplex**

This read-only parameter is set to **Yes**, and specifies full-duplex transmission.

**Physical Port Interface**

The physical port interface is defined by the port's connector and cabling type, and must be configured as follows:

- For the FRX4000 and SmartSwitch 1800, port 0 and port 1 are always RS-232;
- For the FRX4000, ports 2 and 3 are determined by the attached cables: RS-232, V.35, RS-449, or X.21;
- For the SmartSwitch 1800, ports 2 and 3 are determined by the attached cables: RS-232, V.35, or RS-449;
- For the FRX4000, ports 4-7 are determined by the expansion Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, and X.21. (RS-449, and X.21 interfaces require an RS-422 LIC.)
- For the FRX6000, ports 0-7 on each RLP are determined by the Line Interface Card (LIC) and attached I/O cables. Only the valid interfaces will be listed from the menu button. Possible interfaces are: RS-232, V.35, RS-449, RS-530 and X.21. (RS-449, RS-530, and X.21 interfaces require an RS-422 LIC.)

**Blocked Flag**

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or re-booted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed. The default value for this parameter is **No**.

**Generate Clock**

This setting specifies whether the port will generate the clock, or timing, necessary to synchronize traffic over the link. If the port is a physical DCE (as determined by the port's I/O cable interface), specify **Yes**, since the physical DCE generates clock. If the port is a physical DTE, specify **No**. The default value for this parameter is **Yes**.

**Receive Clock from DTE**

This parameter is relevant only if **Physical Port Interface** (see above) is something other than RS-232, and **Generate Clock** (see above) is set to **Yes**. If this parameter is set to **Yes**, it allows the clock (timing) signal to be looped back from the DTE using the Terminal Timing (TT) signal, which can be helpful on high-speed lines.

Generally, if the local interface is a physical DCE and the line speed is above 256 Kbps, this parameter should be set to **Yes**; however, make sure the DTE is configured to provide the terminal timing. The default value for this parameter is **No**.

#### **Clear VC on Last Dev Down**

If **Yes** is selected, this parameter causes the virtual circuit to be cleared when no terminals are using it. The default value for this parameter is **No**.

#### **Pad (Packet Assembler/Disassembler) Type**

You can designate your port as a TPAD (terminal PAD) or an HPAD (host PAD). The default value for this parameter is TPAD.

#### **Answer Non Configured**

This parameter is configurable only if **PAD Type** is HPAD. If you select **Yes**, this parameter will allow the HPAD to respond to all devices on the line. If you select **No**, the HPAD will respond only to those devices that are configured on the node. The default value for this parameter is **Yes**.

#### **Connection Without Poll**

This parameter is configurable only if **PAD Type** is TPAD. If you select **Yes**, this parameter will activate the TPAD connection without a poll of the connected device. If **No** is selected, the TPAD connection will only become activated when the connected device is polled. The default value for this parameter is **Yes**.

## Changing BSCI Port Configuration Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.
3. Click on  to save your changes.

## Applying Port-level Changes

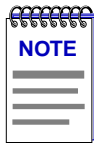
After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## BSCI Subscriber ID Information

The BSCI Subscriber Information window provides information on local and remote subscribers for each BSCI port.

A local TPAD subscriber can specify only one remote device, which can be an HPAD or an X.25 connection to the host. A local HPAD subscriber can specify up to 16 remote devices, any of which can be a TPAD or an X.25 connection to the host. Each connection must be assigned a different local subscriber address.



You must also configure BSCI Device Information for each remote BSC device (see [Configuring BSCI Devices](#), page 8-9).

Use the BSCI Subscriber Information window to configure the subscriber addresses for each of your BSCI ports. To access the window:

1. Click mouse button 3 on the BSCI port of interest to display the Port Menu.
2. Drag down to **BSCI Port Subscriber Configuration**, and release. The BSCI Subscriber Information window, [Figure 8-2](#), will appear.

Local Subscriber	Remote Subscriber	Conn ID	Auto Call	Retry Timer	Retry Count
1234	5678	1	No	60	0

Local Subscriber ID :       Auto Call :  Yes

Remote Subscriber ID :       Retry Timer (15-255) :

Connection ID (0-255) :       Retry Count (0-255) :

Add    Modify    Delete

Refresh    Close

Figure 8-2. BSCI Subscriber Information

The top part of the window displays a list of BSCI port subscribers. The bottom part of the window allows you to modify or add the following BSCI subscriber information:

#### **Local Subscriber ID**

This is the subscriber address of the local end of a BSCI connection. Enter a Subscriber ID of up to 15 digits. This is the same subscriber ID that is specified in the Subscriber Table (see Chapter 4, **Configuring the Subscriber Table**, for Subscriber ID conventions). Each Local Subscriber configured here must also be configured in the Subscriber Table, so that routing information for each subscriber address can be specified.

#### **Remote Subscriber ID**

This is the subscriber address of the remote end of a BSCI connection. It is used by the local device to identify where a call is going. Enter a Subscriber ID of up to 15 digits. A Subscriber ID record must also be configured for this address (see Chapter 4, **Configuring the Subscriber Table** for Subscriber ID conventions).

If the BSCI port is one end of a connection to a logical port in the FRX or SmartSwitch 1800, this ID must match a Subscriber ID configured for the logical port.

#### **Connection ID**

This number identifies the association between a local subscriber and a device configured in the BSCI Device Information window (see **Configuring BSCI Devices**, page 8-9).

#### **Auto Call**

This parameter is relevant only if the **PAD Type** specified for this port is TPAD. If **Yes** is selected, a TPAD will automatically call its HPAD when the Control Unit (CU), identified by the Control Unit ID in the BSCI Device Information window (see **Configuring BSCI Devices**, page 8-9) becomes active. If **No** is selected, no automatic call is placed. If the TPAD is connecting to a logical port in the FRX or SmartSwitch 1800, **Auto Call** must be set to **Yes**. The default value for this parameter is **No**.

#### **Retry Timer**

The amount of time (in seconds) between **Auto Call** retries (see above). If Auto Call is disabled, (if **No** was selected), this field will be grayed out. The default value for this parameter is 60.

#### **Retry Count**

The maximum number of times an **Auto Call** (see above) will be sent. If Auto Call is disabled, (if **No** was selected), this field will be grayed out. The default value for this parameter is 0 (indefinite).

## Adding or Modifying BSCI Subscriber Information

To add a new BSCI Subscriber entry:

1. Enter the **Local Subscriber ID**, the **Remote Subscriber ID**, and the other configurable parameters for the entry.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the Subscriber entry you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you have made some changes but would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the Subscriber entry you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.

## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## Configuring BSCI Devices

After you have configured the port and subscriber information discussed in the previous two sections, you must also define the devices connected to those BSCI ports.

You do this via the BSCI Device Information window. To access the window:

1. Click mouse button 3 on the BSCI port of interest to display the Port Menu.
2. Drag down to **BSCI Device Configuration**, and release. The BSCI Device Information window, [Figure 8-3](#), will appear.



Figure 8-3. BSCI Device Information

The top part of the window displays a list of configured BSCI devices. The bottom part of the window allows you to modify or add the following BSCI device information:

#### Control Unit ID

This ID is a number 0 through 31 and identifies the control unit.

#### Device Unit ID

Enter a number, 0 through 31. Up to 32 Device Units can be configured for each Control Unit.

#### Connection ID

This number identifies the association between a local subscriber on a BSCI port and a device configured here in this table. It must match a **Connection ID** in the BSCI Subscriber Information window (see [BSCI Subscriber ID Information, page 8-7](#)). Valid values are 0 through 255. The default value for this parameter is 0.

#### Single User VC (virtual circuit)

This read-only parameter specifies whether each end of the connection is within a same or different Control Unit/Device Unit pair. This parameter is currently **not** supported and is set to **No**.

**Transparent Text Support**

If **Yes** is selected, then all transmitted characters, including control character sequences, are treated as data. This parameter is useful for transmitting binary data and machine language computer programs without special coding.

Data-link control character sequences transmitted this way must be preceded by a Data Link Escape (DLE) character (a value of 10 in hex) in order to be recognized as control characters.

The default value for this parameter is **No**.

**Printer Attached**

If **Yes** is selected, the device has an attached printer; if **No**, it does not. The default value for this parameter is **No**.

## Adding or Modifying BSCI Device Information

To add a new BSCI Device entry:

1. Enter the **Control Unit ID**, the **Device Unit ID**, and the other configurable values for the entry.
2. Click on  to add your new entry.

To modify an existing Device entry:

1. In the list box, click to select the Device entry you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you have made some changes but would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing Device entry:

1. In the list box, click to select the Device entry you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.

## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.





# IP Interface Configuration

*Configuring IP Node Defaults; IP Interface configuration; Secondary Address configuration*

---

The FRX4000, FRX6000, and the SmartSwitch 1800 support dynamic routing of IP (internet protocol) traffic among IP devices on LANs and routed subnetworks, via frame relay or X.25. The FRX and SmartSwitch 1800 can also be configured to act as IP gateways, forwarding IP packets they receive.

## Configuring IP Node Defaults

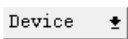
Each FRX or SmartSwitch 1800 device can be configured to support one of three versions of the Routing Information Protocol (RIP). IP uses RIP update messages to send and gather information about the internetwork topology. These update messages are used to construct and maintain routing tables. Routing updates in any of these three RIP versions can be received; however, the device will only transmit updates in the one RIP version you configure.

You can configure the device to transmit one of the three following RIP versions:

- RIP Version 1
- RIP 1 Compatible
- RIP Version 2

RIP Version 1 and RIP Version 2 are incompatible with each other on the same network; however, each is compatible with RIP 1 Compatible. If you are transitioning a network from RIP Version 1 to RIP Version 2, first reconfigure every device to RIP 1 Compatible. When all devices are configured for RIP 1 Compatible, then each device can be configured for RIP Version 2.

You can configure the RIP version for each device through console management, or through the IP Node window. To access the IP Node window:

1. Click on the  button to display the Device menu.
2. Drag down to **IP Node Defaults**, and release. The IP Node window, [Figure 9-1](#), will appear.

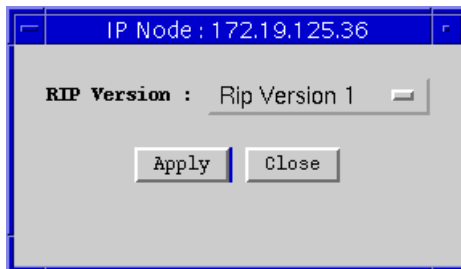

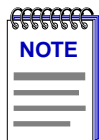


Figure 9-1. The IP Node Window

3. Use the menu button to select the RIP version you want.
4. Click on  to save your selection.

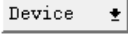


*After you have made system-level changes (such as configuring IP Node Defaults), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Configuring IP Interfaces

An IP interface allows the Internet Protocol to be executed over a frame relay, X.25, Ethernet, or Token Ring interface. You can display all IP interfaces configured on the device and configure a new interface through the IP Interface Configuration window.

To access the IP Interface Configuration window:

1. Click on the  button to display the Device menu.
2. Drag down to **IP Interface Configuration**, and release. The IP Interface Configuration window, [Figure 9-2](#), will appear.

IP Interface Configuration : 172.19.125.34

Interface Number	Interface Type	Priority	Source Address	Destination Address
2	Ethernet Csmacd	5	172.19.125.34	0.0.0.0
21	Frame Relay	5	16.21.20.20	16.21.20.21

Interface Number (1-257) :  Source Subscriber :   
 IP Interface Type :  Destination Subscriber :   
 MTU (1-4096) :  SFC Retry Timer (5-60) :   
 Network Mask :  SFC Idle Timer (0-5) :   
 Route Metric Hops (0-255) :  Max VC (1-8) :   
 ICMP Add Routes :  EVC Connection :   
 RIP Delta Updates (10-300) :  Source RLP (0-7) :   
 RIP Full Updates (10-300) :  Source Port (0-7) :   
 Priority (0-9) :  Source DLCI (16-991) :   
 BAG (1-16) :  RIP Support :   
 Source Address :  Inverse ARP :   
 Destination Address :  Proxy ARP :   
 Broadcast Address :  Unnumbered Interface :   
 LAN Card (0-1) :

Figure 9-2. The IP Interface Configuration Window

The list box at the top of the window displays the IP interfaces that have already been configured; the fields and buttons in the lower portion of the window allow you to add new entries, and modify or delete existing ones.

Following is a description of the IP Interface parameters. The parameters you will configure for each interface depends on the **IP Interface Type** you select (see IP Interface Type definition below).

### Interface Number

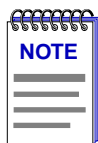
In this field, enter an interface number 1 to 257. This is merely a sequential number used to identify the interface. It is a good idea to configure a LAN interface as interface 0. This ensures that the default IP address used for **Unnumbered Interfaces** (see below) will always be the same.

### IP Interface Type

In this field, use the menu button to select the type of interface you wish to configure. This selection will change the parameters that appear in the IP Interface Configuration window. Depending on your selection, certain parameters will be configurable, and others will be grayed out.

There are five IP interface types that you can select from:

- Rfc 877x25 (X.25)
- Ethernet Csmacd (Ethernet II)
- Iso 88023 Csmacd
- Iso 88025 Token Ring
- Frame Relay



*The Ethernet and Token Ring IP Interface types will be referred to collectively as LAN interfaces.*

### Maximum Transmission Unit

This is the maximum size (in bytes) of the data field that can be used to encapsulate an IP datagram for transmission over the interface. Any datagrams larger than the Maximum Transmission Unit will be fragmented, resulting in additional processing on any intermediate routers or gateways, as well as the destination host. If the maximum Transmission Unit value is less than the size of a minimal IP datagram, the value will automatically change to the minimal datagram size. The default value for this parameter is 1500.

### Network Mask

This field is used during routing to determine the portion of the IP address associated with the network and subnetwork (if any). The valid entries are 255.0.0.0 to 255.255.255.255 (255.255.255.255 is only valid on a point-to-point interface).

The default value for this parameter is configured automatically to reflect the appropriate address class for the specified **Source Address** (see below). If the Source IP Address is changed, the Network Mask will automatically change to a default value appropriate for the new address. For this reason, configure the Source IP Address first, then the Network Mask.

If the interface is configured as an **Unnumbered Interface** (see below), the default value of Network Mask will be based on the numbered interface that is assigned.

### Route Metric Hops

This is the number of network hops (network gateways in the overall path over the internet) associated with this interface (usually zero). During routing, the interface with the lowest count will be selected. The default value for this parameter is 0.

**ICMP Add Routes**

Select **Yes** or **No** to specify whether IP may add routes obtained by ICMP (Internet Control Message Protocol). ICMP's error and control function is used to send redirection options back to the source, if problems are discovered. The default value for this parameter is **Yes**.

**RIP Delta Updates**

This field specifies (in seconds) the frequency with which RIP update messages will be sent to every neighbor node. These messages contain any changes to the routing table that occurred since the last **RIP Full Update** (see next definition). The default value for this parameter is 10.

**RIP Full Updates**

This field specifies (in seconds) the frequency with which updates of the entire routing table will be sent to every neighbor node, via one or more RIP messages. The default value for this parameter is 30.

**Priority**

This field prioritizes the interface for traffic within the device; the higher the number, the higher the priority. This priority has no effect on traffic exiting the device. Priorities are configured on all logical interfaces that use a physical frame relay port. The FRX or SmartSwitch 1800 processor uses these priorities to help determine the order in which it will process protocols. The default value for this parameter is 5.

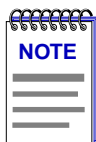


*When configuring priorities, be sure to consider the types of traffic being routed on other connections in the node.*

**BAG**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It assigns the IP interface to one of 16 Bandwidth Allocation Groups (BAG).

BAGs regulate bandwidth usage by outgoing traffic on the physical link and can ensure that response time-sensitive traffic gets access to the available frame relay bandwidth. Up to 16 groups can be configured through console management (refer to your FRX or SmartSwitch 1800 hardware documentation for more information).



*Bandwidth allocation groups cannot currently be configured via SPMA; for more information on configuring these groups, see your FRX or SmartSwitch 1800 hardware documentation.*

### Source Address

This is the IP address of the end-to-end sender (the IP interface). The valid range of values (1.0.0.0 to 223.255.255.255) guarantees that you cannot configure all 0s or all 1s for a network ID, node ID, or subnet ID. If the interface is configured as an **Unnumbered Interface** (see below), you will **not** enter a source address here.

### Destination Address

This parameter is only configurable when the **Interface Type** is X.25, or when the **Interface Type** is Frame Relay and the **Inverse ARP** parameter is Disabled. It is the IP address of the end-to-end receiver for point-to-point connections. The valid range of values (1.0.0.0 to 223.255.255.255) guarantees that you cannot configure all 0s or all 1s for a network ID, node ID, or subnet ID.

### Broadcast Address

If you specified a LAN **Interface Type**, use this field to designate the address used to send broadcast messages to all LAN hosts on the network. The default value of the broadcast address will be configured automatically after a **Source Address** or **Network Mask** is specified (see above). The value will be the dotted decimal notation result of “ANDing” the binary versions of the Source Address and the Network Mask, then filling in the remaining bits with 1s.

If the Source Address or Network Mask is changed, the associated broadcast address will automatically change to the default value appropriate for the new address. For this reason, configure the Source Address first, then the Network Mask, then the Broadcast Address.

### LAN Card

If you specified a LAN **Interface Type**, this number identifies the LAN card that contains the IP interface. Enter 0 for the FRX4000 or SmartSwitch 1800; 0 or 1 for the FRX6000.

### Source Subscriber

This parameter is only configurable if you have selected X.25 as your **Interface Type**. This is the Subscriber ID associated with the source IP interface port. A subscriber ID is an address of up to 15 digits. This address must also be configured in the Subscriber Table (see Chapter 4, **Configuring the Subscriber Table**), and cannot contain wildcards. When configuring the Subscriber Table for the source subscriber, do not configure any routing path in the Routing Table.

### Destination Subscriber

This parameter is only configurable if you have selected X.25 as your **Interface Type**. This is the Subscriber ID associated with the destination IP interface port. A subscriber ID is an address of up to 15 digits. This address must also be configured in the Subscriber Table (see Chapter 4, **Configuring the Subscriber Table**), and cannot contain wildcards. When configuring the Subscriber Table for the destination subscriber, configure the first routing path as the RLP and X.25 port that will be used for the physical interface. (On an FRX6000, that RLP does not need to be the same one that has IP installed.)

**SVC Retry Timer**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. It specifies the time (in seconds) between calls that are placed to try to establish an X.25 connection. The default value for this parameter is 20.

**SVC Idle Timer**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. It specifies the amount of time (in minutes) that IP will remain active with no traffic, before the X.25 connection is cleared. The default value for this parameter is 1.

**Max VC**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. It specifies the maximum number of virtual circuits over which IP traffic will be transmitted in parallel. The default value for this parameter is 1.

**PVC Connection**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. Select **Yes** if the interface is a Permanent Virtual Circuit (PVC); select **No** if it is not. The default value for this parameter is **No**.

**Source RLP**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It identifies the RLP for the logical interface at this end of the frame relay link. Enter 0 for FRX4000 and SmartSwitch 1800 devices (for RLP0); enter 0 - 7 for an FRX6000.

**Source Port**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It identifies the physical frame relay port for the logical interface at this end of the frame relay link. Make sure the physical frame relay port you identify is not configured for backup use only.

**Source DLCI**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It identifies the DLCI for the logical interface at this end of the frame relay link. Make sure the DLCI you identify is not part of a frame relay DLCI backup group or intra-nodal frame relay PVC.

**RIP Support**

This field specifies the level of RIP support on the interface. If you select Enabled, all RIP messages will be accepted, and messages of the RIP version configured in IP Node Defaults (see [page 9-1](#)) will be transmitted. If you select Disabled, no RIP messages will be accepted or transmitted. If you select Receive Only, RIP messages will be accepted, but not transmitted. The default value for this parameter is Enabled.

### Inverse ARP

By selecting Enabled in the Inverse ARP field, you can configure a frame relay interface without specifying a destination IP address. Once the frame relay interface and its DLCI become active, the IP function in the FRX or SmartSwitch 1800 device sends an Inverse ARP (Address Resolution Protocol) request over the interface. The response will contain the destination IP address, allowing the IP interface to become active.

If an ARP request from the FRX or SmartSwitch 1800 receives no response within five seconds, the request will be resent every five seconds for an additional five times. If there is still no response, a 30-second timer will start. When the timer expires, the resend sequence will be repeated.

If you have upgraded your firmware to version 4.0, then the default value for IP interfaces that have already been configured is Disabled. If you are adding a new interface, the default value is Enabled. If you select Disabled, you must enter a **Destination Address** (see definition above).

If Inverse ARP is changed from Enabled to Disabled, the device will immediately generate an Inverse ARP request.

### Proxy ARP

This parameter is only configurable if you have selected a LAN interface as your **Interface Type**, and determines whether Proxy ARP (Address Resolution Protocol) will be supported. Proxy ARP allows an FRX or SmartSwitch 1800 to respond to ARP requests on one subnet for a host on another subnet. The device that sent the ARP request thinks the FRX or SmartSwitch 1800 is the destination host.

If an ARP request is received, the IP function in the FRX or SmartSwitch 1800 checks the address against the **Source Address** configured on the IP interface. If the addresses match, a reply will be sent. If the addresses do not match, and Proxy ARP is Disabled, no response will be sent. If the addresses do not match, and Proxy ARP is Enabled, the IP function will check to see if the device has a route to the host or the host's network. If there is a route, and the route is reachable and is not on the same interface on which the ARP request was received, an ARP response will be sent.

The default value for this parameter is Disabled.

### Unnumbered Interface

This parameter is only configurable if you have selected Frame Relay or X.25 as your **Interface Type**. It allows a point-to-point frame relay interface to be configured without specifying a **Source Address** (see above). If **Yes** is selected, the address of the lowest **Interface Number** in the FRX or SmartSwitch 1800 is used as a default source IP address. (The lowest Interface Number is **not** the lowest address, but the lowest number, in the range 1 - 257, that identifies the interface.) It doesn't matter what type the interface is. All unnumbered interfaces on the device will use the same default source IP address.

If a new interface with a lower number is added, that interface's IP address will become the new default source IP address, but only after you reboot the device.



This function will only work if there is at least one numbered interface in the device. If there isn't one, all unnumbered interfaces will remain disabled until a numbered interface is added.

If you have upgraded your firmware to version 4.0, then the default value for IP interfaces that have already been configured is **No**. If you are adding a new interface, the default value is **Yes**. If you select **No**, you must enter a **Source Address** (see definition above).

## Configuring IP Interface Secondary Addresses

If you have selected a LAN interface as your **Interface Type** in the IP Interface Configuration window, you can use the **Secondary** button at the bottom of the window to access the IP Interface Secondary Address Configuration window.

This window allows you to configure up to 15 secondary IP addresses on a LAN interface, providing support for multiple IP subnets on the same physical LAN segment.

To access the IP Interface Secondary Address Configuration window, click on the **Secondary** button at the bottom of the IP Interface Configuration window. The IP Interface Secondary Address Configuration window, [Figure 9-3](#), will appear.

Seq	Network Mask	Hops	Source Address	Broadcast Address	RIP Support

Sequence Number(1-15) :       Source Address :   
 Network Mask :       Broadcast Address :   
 Route Metric Hops (0-255) :       RIP Support : Disabled

Figure 9-3. The IP Interface Secondary Address Configuration

The list box at the top of the window displays the Secondary Addresses that have already been configured; the fields and buttons in the lower portion of the window allow you to add new entries and modify or delete existing ones.

Following is a description of the Secondary Address parameters:

### **Sequence Number**

In this field, enter a number (1 to 15) to identify the secondary address. The default value is the next number in sequence.

### **Network Mask**

This field is used during routing to determine the portion of the IP address associated with the subnetwork. The valid entries are 255.0.0.0 to 255.255.255.255 (255.255.255.255 is only valid on a point-to-point interface).

The default value for this parameter is configured automatically to reflect the appropriate address class for the specified secondary **Source Address** (see below). If the secondary Source IP Address is changed, the Network Mask will automatically change to a default value appropriate for the new address. For this reason, configure the secondary Source IP Address first, then the Network Mask.

### **Route Metric Hops**

This field specifies the routing metric count associated with the secondary IP address. This is the number of hops (subnet gateways in the overall path over the internet) associated with this interface (usually zero). During routing, the interface with the lowest count will be selected. The default value for this parameter is 0.

### **Source Address**

This field specifies the secondary IP address. The valid range of values (1.0.0.0 to 223.255.255.255) guarantees that you cannot configure all 0s or all 1s for a network ID, node ID, or subnet ID.

### **Broadcast Address**

This is the broadcast address associated with the secondary IP address. This address is used to send broadcast messages to all LAN hosts on the subnetwork.

The default value of the broadcast address will be configured automatically after a secondary **Source Address** or **Network Mask** is specified (see above). The value will be the dotted decimal notation result of “ANDing” the binary versions of the Source Address and the Network Mask, then filling in the remaining bits with 1s.

If the secondary Source Address or Network Mask is changed, the associated broadcast address will automatically change to the default value appropriate for the new address. For this reason, configure the Source Address first, then the Network Mask, then the Broadcast Address.

### RIP Support

This field specifies the level of RIP support for the secondary IP address. If you select Enabled, all RIP messages will be accepted, and messages of the RIP version configured in IP Node Defaults (see [page 9-1](#)) will be transmitted. If you select Disabled, no RIP messages will be accepted or transmitted. If you select Receive Only, RIP messages will be accepted, but not transmitted. The default value of this parameter is Enabled.

## Adding or Modifying IP Interfaces

First, access the IP Interface Configuration window (see [Configuring IP Interfaces, page 9-2](#)).

To add a new IP interface:

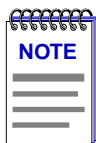
1. Enter the **IP Interface Number**, the **IP Interface Type**, and the other configurable values for each interface.
2. Click on  to add your new entry.

To modify an existing entry:

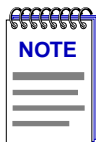
1. In the list box, click to select the IP Interface you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the IP Interface you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring an IP Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*




*If you want to delete an interface without deleting a group of associated secondary addresses, you must first select one of the secondary addresses to be the new **Source Address** and delete that secondary address (see [Adding or Modifying Secondary Addresses](#)). Then, modify the **Source Address** parameter to specify the secondary address that was deleted.*

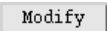
## Adding or Modifying Secondary Addresses

If you have specified a LAN Interface as your IP Interface Type, you can access the IP Interface Secondary Address Configuration window by clicking on the **Secondary** button at the bottom of the IP Interface Configuration window.


To add a new IP interface Secondary Address:

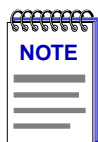
1. Enter the **Sequence Number**, the **Source Address**, and the other configurable values for the secondary address.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the IP Interface Secondary Address you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the IP Interface Secondary you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring an IP Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

# IPX Interface Configuration

*Configuring IPX Node Defaults; IPX Interface configuration; IPX Static SAP and Static Route configuration*

---

The FRX4000, FRX6000, and the SmartSwitch 1800 support connections to Novell IPX networks through an IPX (Internet Packet Exchange) Interface. IPX is the Novell proprietary protocol that specifies how information is to be broken into separate packets, and how those packets are to be addressed in order to be routed from one Novell NetWare node to another, and from one Novell NetWare network to another. The IPX interface enables the FRX or SmartSwitch 1800 to route IPX traffic between local LANs, or between LAN-attached workstations and local or remote servers, via frame relay or X.25.

## Configuring IPX Node Defaults

If the FRX4000, FRX6000, or SmartSwitch 1800 is going to support an IPX interface, certain IPX node parameters must be configured through the IPX Node Defaults window.

To access the IPX Node Defaults window:

1. Click on the **Device** button to display the Device menu.
2. Drag down to **IPX Node Defaults**, and release. The IPX Node Defaults window, [Figure 10-1](#), will appear.

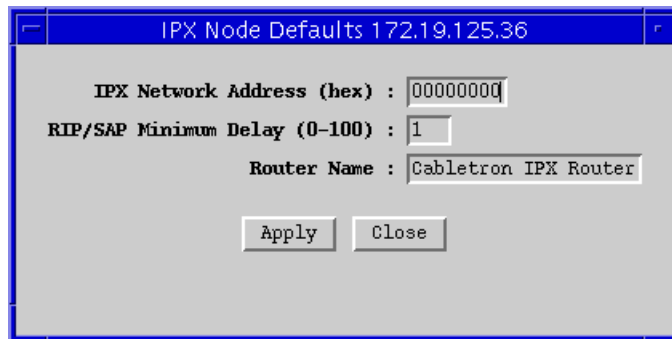
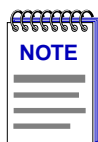


Figure 10-1. The IPX Node Defaults Window

3. In the **IPX Network Address** field, enter an 8-digit hexadecimal address to identify the node to the IPX network.
4. In the **RIP/SAP Minimum Delay** field, enter the minimum delay (in 55 millisecond intervals) between consecutive Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) transmissions. This parameter provides compatibility with older Novell servers. The default value for this parameter is 1.
5. In the **Router Name** field, enter a router name (up to 48 characters) which serves as an identifier for the IPX network. It must be unique within the network. You can enter up to 48 characters, but you can only view 20 characters at a time.
6. Click on  to save your selections.



*After you have made system-level changes (such as configuring IPX Node Defaults), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Configuring IPX Interfaces

An IPX interface allows an FRX4000, FRX6000, and SmartSwitch 1800 to connect to a Novell IPX network. You can display all IPX interfaces configured on the device and configure a new interface through the IPX Interface Configuration window.

To access the IPX Interface Configuration window:

1. Click on the  button to display the Device menu.

2. Drag down to **IPX Interface Configuration**, and release. The IPX Interface Configuration window, [Figure 10-2](#), will appear.

The screenshot shows the 'IPX Interface Configuration : 172.19.125.36' window. At the top, there is a table with three columns: 'Interface Number', 'Interface Type', and 'Network Address'. Below this table is a large empty list box. The lower portion of the window contains various configuration fields and buttons.

Interface Number	Interface Type	Network Address

Configuration Parameters:

- Interface Number (1-64) : 1
- Interface Type : Ethernet
- Network Address : 00000000
- Frame Type : Type II
- MTU (45-1518) : 1518
- BAG (1-16) : 1
- LAN Card (0,1) : 0
- Source Subscriber :
- Dest. Subscriber :
- SVC Retry Timer (5-60) :
- SVC Idle Timer (0-5) :
- Blocked Flag : No
- Diagnostics Enabled : No
- Serialization Enabled : No
- WAN Enabled : No
- NetBIOS Enabled : No
- Periodic SAP Enabled : No
- SAP Enabled : No
- Periodic RIP Enabled : No
- RIP Enabled : No
- Watchdog Spoofing : No
- EVC Connection : No
- Source RLP (0-7) :
- Source Port (0-7) :
- Source DLCI (16-991) :
- Transport Time (1-255) : 1
- NetBIOS Hops (0-255) : 8
- Periodic SAP Timer (1-65535) : 60
- SAP Age Timer (0-65535) : 180
- Periodic RIP Timer (1-65535) : 60
- RIP Age Timer (0-65535) : 180
- RIP Max Size (54-446) : 446
- Max VC (1-8) :

Buttons: Add, Modify, Delete, Refresh, Close

Figure 10-2. The IPX Interface Configuration Window

The list box at the top of the window displays the IPX interfaces that have already been configured; the fields and buttons in the lower portion of the window allow you to add new entries, and modify or delete existing ones.

Following is a description of the IPX Interface parameters. Which parameters you will configure for each interface depends on the **IPX Interface Type** you select (see IPX Interface Type definition below).

#### Interface Number

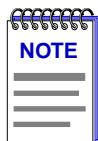
In this field, enter an interface number 1 to 64. This is merely a sequential number used to identify the interface.

### Interface Type

In this field, use the menu button to select the type of interface you wish to configure. Depending on your selection, certain parameters will be configurable, and others will be grayed out.

There are four IPX interface types that you can select from:

- Ethernet
- Eight 025 (Token Ring)
- X.25
- Frl (Frame Relay)



*The Ethernet and Token Ring IPX Interface types will be referred to collectively as LAN interfaces.*

### Network Address

This field identifies the local interface to the Novell network. Enter an address up to 10 digits in length.

### Frame Type

This field depends on the **Interface Type** you have selected. If you have selected Ethernet or Token Ring as your interface type, you can use the menu button to select one of the following four frame types: Type II, Raw, Llc, or Snap. If you have selected Frame Relay or X.25 as your interface type, your only option is Type II.

### Maximum Transmission Unit

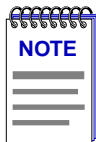
This is the maximum frame size (in bytes) that can be transmitted or received over the IPX interface. Valid values for frame relay or X.25 interface types are 31 to 4096 bytes; valid values for Ethernet interface types are 45 to 1518 bytes, and valid values for Token Ring interfaces are 48 to 4096 bytes. The default value for each interface type is the highest amount.

### BAG

This parameter assigns the IPX interface to one of 16 Bandwidth Allocation Groups (BAG).

BAGs regulate bandwidth usage by outgoing traffic on the physical link and can ensure that response time-sensitive traffic gets access to the available frame relay bandwidth. Up to 16 groups can be configured through console management (refer to your FRX or SmartSwitch 1800 hardware documentation for more information).





*Bandwidth allocation groups cannot currently be configured via SPMA; for more information on configuring these groups, see your FRX or SmartSwitch 1800 hardware documentation.*

### **LAN Card**

If you specified a LAN **Interface Type**, this number identifies the LAN card that contains the IPX interface. Enter 0 for the FRX4000 or SmartSwitch 1800; 0 or 1 for the FRX6000.

### **Source Subscriber**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. This is the Subscriber ID that defines an IPX interface in the node, by associating itself with port 66, a number reserved for the IPX interface.

A subscriber ID is an address of up to 15 digits. This address must also be configured in the Subscriber Table (see Chapter 4, **Configuring the Subscriber Table**).

### **Destination Subscriber**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. This is the Subscriber ID associated with the physical X.25 port that will be used for the IPX interface.

A subscriber ID is an address of up to 15 digits. This address must also be configured in the Subscriber Table (see Chapter 4, **Configuring the Subscriber Table**).

### **SVC Retry Timer**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. It specifies the time (in seconds) between calls that are placed to try to establish an X.25 connection. The default value for this parameter is 20.

### **SVC Idle Timer**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. It specifies the amount of time (in minutes) that an IPX connection can remain active with no traffic, before the connection is cleared. The default value for this parameter is 1.

### **Blocked Flag**

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or re-booted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed. The default value for this parameter is **No**.

### **Diagnostics Enabled**

This parameter determines the IPX interface's ability to handle Novell diagnostic packets. If **Yes** is selected, IPX will forward or respond to a diagnostic packet depending on the packet's address. If **No** is selected, the IPX interface will ignore Novell diagnostic packets. The default value for this parameter is **No**.

### **Serialization Enabled**

This parameter determines whether NetWare file server serialization security frames will be forwarded on the interface. These broadcast frames are used by Novell to hold information regarding the licensing of the file server executables.

If **Yes** is selected, these frames will be forwarded; if **No**, they will not. Selecting **No** allows filtering of these broadcasts to reduce WAN traffic, and is not intended to interfere with copyright-protection mechanisms. The default value for this parameter is **No**.

### **WAN Enabled**

This parameter is configurable only if you have selected Frame Relay or X.25 as your **Interface Type**. It determines whether Novell's IPXWAN protocol will be used (if **Yes**) or not (if **No**) on the IPX interface. IPXWAN specifies a method for IPX routers to communicate across WAN links. The default value for this parameter is **No**.

### **NetBIOS Enabled**

This parameter determines whether Novell-encapsulated NetBIOS frames received on the IPX interface will be processed (if **Yes**) or discarded (if **No**). The default value for this parameter is **No**.

### **Periodic SAP Enabled**

This field determines whether the FRX or SmartSwitch 1800 will originate periodic IPX Service Advertising Protocol (SAP) messages from this interface. (The **SAP Enabled** parameter must be set to **Yes**, see below). These messages inform the network which SAP entries in the routing table are viable. The default value for this parameter is **No**.

### **SAP Enabled**

If **Yes** is selected, the IPX interface will support Service Advertising Protocol (SAP) processing; if **No**, it will not. SAP is used by IPX to exchange information about Novell service-providing nodes, such as file servers and print servers that are available. SAP builds and maintains a database, the Service Advertisement Table, containing the addresses of and routes to specific service-providing nodes (servers), and advertises this information over the network. The default value for this parameter is **No**.

**Periodic RIP Enabled**

This field determines whether the FRX or SmartSwitch 1800 will originate periodic IPX Routing Information Protocol (RIP) messages from this interface. (The **RIP Enabled** parameter must be set to **Yes**, see below). These messages inform the network that the route through this interface is viable. The default value for this parameter is **No**.

**RIP Enabled**

If **Yes** is selected, the IPX interface will support Routing Information Protocol (RIP) processing; if **No**, it will not. RIP is the routing protocol used by IPX to build and maintain routing tables which contain the addresses of and available routes to all the networks and nodes RIP has learned. The default value for this parameter is **No**.

**Watchdog Spoofing**

This field determines whether this IPX interface will be used by the local node to respond to keep-alive messages on behalf of the client workstations. Novell servers periodically issue these messages to all clients, to determine whether each client is still available. The default value for this parameter is **No**.

**PVC Connection**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. Select **Yes** if the interface is a Permanent Virtual Circuit (PVC); select **No** if it is not. The default value for this parameter is **No**.

**Source RLP**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It identifies the RLP for the IPX interface at this end of the frame relay link. Enter 0 for FRX4000 and SmartSwitch 1800 devices (for RLP0); enter 0 - 7 for an FRX6000.

**Source Port**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It identifies the physical frame relay port for the IPX interface at this end of the frame relay link. Make sure the physical frame relay port you identify is not configured for backup use only as determined by the **Backup Use Only** parameter in the Frame Relay Port Configuration window. (See Chapter 5, Frame Relay Status and Configuration.)

**Source DLCI**

This parameter is only configurable if you have selected Frame Relay as your **Interface Type**. It identifies the DLCI for the IPX interface at this end of the frame relay link. Make sure the DLCI you identify is not part of a frame relay DLCI backup group or intra-nodal frame relay PVC.

**Transport Time**

This is the time (in 55-millisecond units) that it will normally take to forward frames out the IPX interface. Recommended values are 1 for LAN interfaces and 30 for frame relay or X.25 interfaces. The default value for this parameter is 1. This

time is used to calculate the least-cost path during routing. If **WAN Enabled** is set to **Yes** (see above), the Transport Time selected here will be overridden by the value calculated by IPXWAN.

#### **NetBIOS Hops**

This is the maximum number of network hops allowed for routing a Novell-encapsulated NetBIOS frame. Each router in a packet's path to the destination network is one hop. Frames exceeding this value will be discarded. The default value for this parameter is 8.

#### **Periodic SAP Timer**

If **Periodic SAP Enabled** is set to **Yes** (see above), then this field specifies the interval (in seconds) between the periodic IPX Service Advertising Protocol (SAP) broadcasts from this interface. If this is set to greater than 0, the **SAP Age Timer** (see below) must be three times longer than the Periodic SAP Timer. The default value for this parameter is 60.

#### **SAP Age Timer**

If **SAP Enabled** is set to **Yes** (see above), this timer is used to delete route entries in the server information table. The timer starts each time SAP creates or updates an entry, or an entry is referenced for forwarding. This field specifies the amount of time (in seconds) that will elapse before the timer expires and the router assumes that the entry is no longer valid (due to hardware failure, power outage, etc.), and the entry will be deleted from the table. SAP will then send a broadcast message indicating that the server is down. If the value for the Periodic SAP Timer is set to greater than 0, the SAP Age Timer must be three times longer than the Periodic SAP Timer. A value of 0 for the SAP Age Timer disables aging. The default value for this parameter is 180.

#### **Periodic RIP Timer**

If **Periodic RIP Enabled** is set to **Yes** (see above), then this field specifies the interval (in seconds) between the periodic IPX Routing Information Protocol (RIP) broadcasts from this interface. If this is set to greater than 0, the **RIP Age Timer** (see below) must be three times longer than the Periodic RIP Timer. The default value for this parameter is 60.

#### **RIP Age Timer**

If **RIP Enabled** is set to **Yes** (see above), this timer is used to delete route entries in the routing information table. The timer starts each time an entry is created, updated, or referenced for forwarding by RIP. This field specifies the amount of time (in seconds) that will elapse before the timer expires and the router assumes that the entry is no longer valid (due to hardware failure, power outage, etc.) and the entry will be deleted from the table. If the value for the Periodic RIP Timer is set to greater than 0, the RIP Age Timer must be three times longer than the Periodic RIP Timer. A value of 0 for the RIP Age Timer disables aging. The default value for this parameter is 180.

**RIP Max Size**

This is the maximum RIP packet size (in bytes), including the IPX header (30 bytes) and the LAN MAC header (if transmitted on a LAN interface). The default value for this parameter is 446.

**Max VC**

This parameter is only configurable if you have selected X.25 as your **Interface Type**. It specifies the maximum number of virtual circuits over which IPX traffic will be transmitted in parallel. The default value for this parameter is 1.

## Adding or Modifying IPX Interfaces

First, access the IPX Interface Configuration window (see [Configuring IPX Interfaces](#), page 10-2).

To add a new IPX interface:

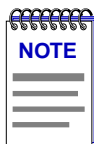
1. Enter the **IPX Interface Number**, the **IPX Interface Type**, and the other configurable values for each interface.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the IPX Interface you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the IPX Interface you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring an IPX Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Configuring IPX Static Routes

The routing of IPX traffic is handled dynamically using RIP routing tables and SAP service advertisement tables as discussed in the previous section. However, you can also configure static routes for IPX traffic using the IPX Static SAP Configuration window and the IPX Static Route Configuration window.

These two windows and their parameters are described in the following sections.

### IPX Static SAP Configuration

To access the IPX Static SAP Configuration window:

1. Click on the **Device** button to display the Device menu.
2. Drag down to **IPX Static SAP Configuration**, and release. The IPX Static SAP Configuration window, [Figure 10-3](#), will appear.

Service Type	Service Name	Net Address	Node Address	Socket	Hops	Gateway Address	Interface
--------------	--------------	-------------	--------------	--------	------	-----------------	-----------

Service Type :  Socket Number (0-65535) :

Service Name :  Intervening Networks (1-65535):

Network Address :  Gateway Address :

Node Address :  Interface (0-65535) :

Figure 10-3. The IPX Static SAP Configuration Window

The list box at the top of the window displays the IPX static routes that have already been configured; the fields and buttons in the lower portion of the window allow you to add new entries, and modify or delete existing ones.

Following is a description of the IPX Static Route parameters that you can configure:

**Service Type**

This field is a SAP Service Type code. Some common types are:

0003 = print queue	0007 = print server
0004 = file server	0009 = archive server
0005 = job server	0024 = remote bridge server

**Service Name**

Identifies a specific server in the IPX network. Enter a name of 1-48 characters; the default value of this parameter is \* (asterisk), a wildcard character.

**Network Address**

This is an IPX network number assigned to the network containing the server identified by **Service Name**.

**Node Address**

This address identifies the IPX node attached to the server network.

**Socket Number**

The IPX socket number that identifies the process. For example, the SAP process is 0452. The default value for this parameter is 0.

**Intervening Networks**

The number of routers that a packet must pass through to reach the server, if this route is used. The default value for this parameter is 1.

**Gateway Address**

The hex value of the node address of the router that will forward a packet when this route is used. If Novell's IPXWAN protocol is used on the interface (as configured in the IPX Interface Configuration window; see [page 10-2](#)), this field is ignored.

**Interface**

This is the IPX network number assigned to the interface used to send packets that are destined for this server.


**Adding or Modifying Static SAP Routes**

First, access the IPX Static SAP Configuration window (see [IPX Static SAP Configuration, page 10-10](#)).


To add a new Static SAP route:

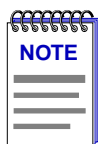
1. Enter the **Service Type**, the **Service Name**, and the other configurable values for each route.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the Static SAP Route you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

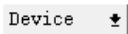
1. In the list box, click to select the Static SAP Route you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring an IPX Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## IPX Static Route Configuration

To access the IPX Static Route Configuration window:

1. Click on the  button to display the Device menu.
2. Drag down to **IPX Static Route Configuration**, and release. The IPX Static Route Configuration window, [Figure 10-4](#), will appear.



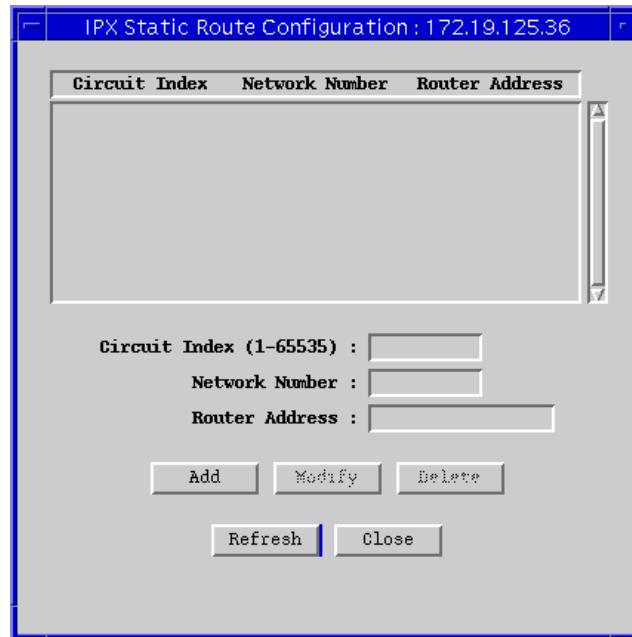


Figure 10-4. The IPX Static Route Configuration Window

The list box at the top of the window displays the IPX static routes that have already been configured; the fields and buttons in the lower portion of the window allow you to add new entries, and modify or delete existing ones.

Following is a description of the IPX Static Route parameters that you can configure:

**Circuit Index**

This number is the unique identifier of the circuit used to reach the first hop in the static route.

**Network Number**

Enter the IPX network number of the route's destination.

**Router Address**

Enter the hex value of the node address of the router that will forward a packet when this route is used. If Novell's IPXWAN protocol is used on the interface (as configured in the IPX Interface Configuration window; see [page 10-2](#)), this field is ignored.

## Adding or Modifying IPX Static Routes

First, access the IPX Static Route Configuration window (see [IPX Static Route Configuration](#), page 10-12).

To add a new IPX Static Route:

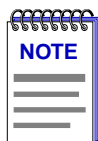
1. Enter the **Circuit Index**, the **Network Number**, and the **Router Address** for each route.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the static route you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the static route you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring an IPX Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

# Bridge Configuration

*About FRX and SmartSwitch 1800 Bridging support; configuring device-level bridging parameters; configuring bridge ports on frame relay and LAN interfaces*

---

The FRX and SmartSwitch 1800 devices support bridging of LAN traffic over Frame Relay. This bridging support includes:

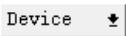
- encapsulation of Ethernet and Token Ring traffic (per RFC 1490) for transmission over Frame Relay
- Transparent Spanning Tree (802.1d) bridging
- compatibility with Source Route Bridging environments
- translational bridging between Ethernet and Token Ring LANs
- bridging of IP and IPX traffic.

Bridging is supported on Ethernet, Token Ring, and Frame Relay interfaces.

## Configuring Device-Level Bridging Parameters

If the FRX4000, FRX6000, or SmartSwitch 1800 is going to support one or more bridge ports (interfaces), certain device-level bridging parameters must be configured to define bridge operation.

Using the Bridge Configuration window, you can configure the device-level bridging parameters. To access the window:

1. Click on  to display the Device menu.
2. Drag down to **Bridge Configuration**, and release. The Bridge Configuration window, [Figure 11-1](#), will appear.

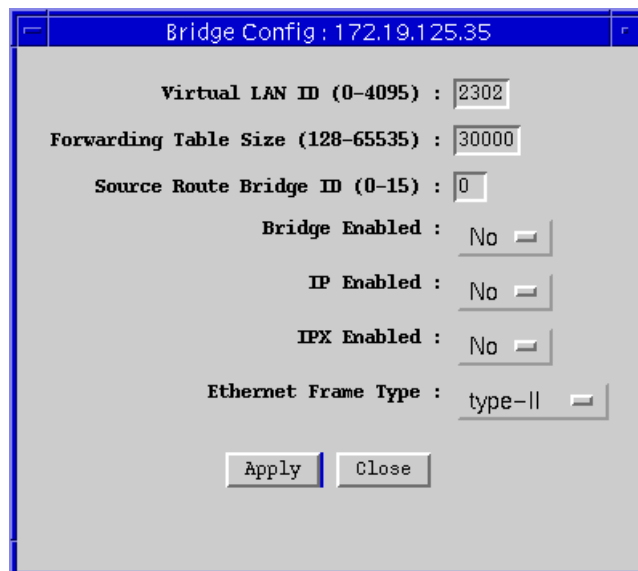


Figure 11-1. Bridge Configuration

You can configure the following bridging parameters:

#### Virtual LAN ID

This ID is only used in an 802.5 Source Route environment and is normally assigned by a system administrator. It is the ID number that is inserted into the Token Ring RIF field representing the internal virtual ring for LLC2 or bridged traffic.

Each Virtual LAN ID must be unique among all LAN IDs throughout the network on which this device will operate.

#### Forwarding Table Size

Under the Spanning Tree concept, bridges automatically maintain forwarding tables by exchanging messages (BPDUs) with other bridges on the network. By using the information in the forwarding tables, bridges determine single paths for traffic between endpoints (assuming there are multiple paths.)

This field determines the maximum number of entries allowed in the bridge's forwarding table. The actual number may be limited by available memory. The default value for this parameter is 65535.

#### Source Route Bridge ID

This ID is only used in a 802.5 Source Route environment. If the outgoing port is configured as a Source Route bridge, it is necessary for the FRX or SmartSwitch 1800 to generate the Routing Information Field (RIF) in forwarded frames. This Bridge ID supplies the Source Route Bridge ID that will be inserted into the RIF.

The default value for this parameter is 0. The Bridge ID must be 0 if the bridge port is on an IBM Token Ring card.

**Bridge Enabled**

If **Yes** is selected, bridging is in effect, and all traffic types are allowed on the bridge interface. If **No** is selected, only LLC2 terminated traffic is allowed on the bridge interface. The default value for this parameter is **Yes**.

**IP Enabled**

If **Yes** is selected, IP traffic will be bridged. If **No** is selected, IP bridging is not enabled, and IP traffic (assuming IP is configured and loaded in the FRX or SmartSwitch 1800) will be routed. The default value for this parameter is **No**.

**IPX Enabled**

If **Yes** is selected, IPX traffic will be bridged. If **No** is selected, IPX bridging is not enabled, and IPX traffic (assuming IPX is configured and loaded in the FRX or SmartSwitch 1800) will be routed. The default value for this parameter is **No**.

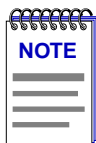
**Ethernet Frame Type**

This selection determines the Ethernet frame type that will be used in Token Ring to Ethernet translation. If the FRX or SmartSwitch 1800 does not know the frame type generated by the attached Ethernet device, it will check this field to determine what Ethernet frame type to use. However, once the FRX or SmartSwitch device has received a frame from a device over the Ethernet interface, it will know what format to use for future frames. Select type-II for Ethernet Type II frame type; select ieee8023 for IEEE 802.3 Ethernet frame type. The default value for this parameter is type-II. This parameter is irrelevant on Token Ring FRX4000 and SmartSwitch 1800 devices.

## Changing Configuration Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.
3. Click on  to save your changes.



*After you have made system-level changes (such as configuring a Bridge Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Configuring Bridge Ports


An FRX or SmartSwitch 1800 bridge port is a LAN interface or a frame relay port that will operate as a bridge connection to the LAN or WAN respectively. There are two windows provided to configure bridge ports:

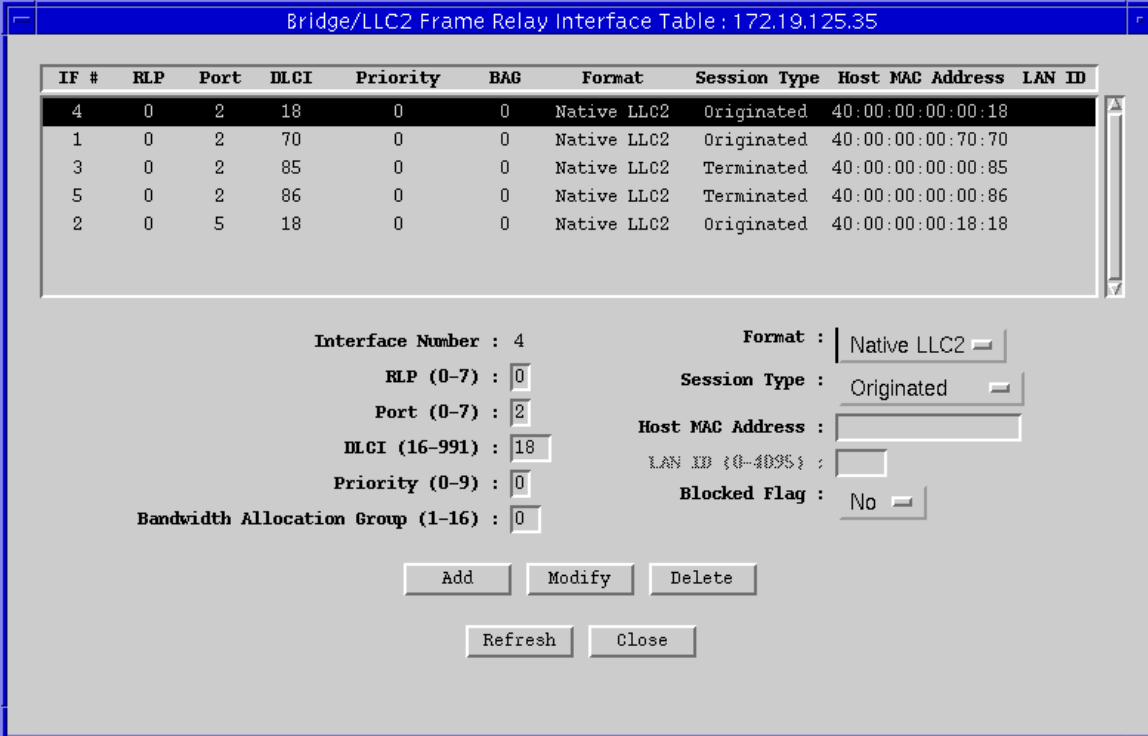
- The **Bridge/LLC2 Frame Relay Interface Table** allows you to configure a frame relay port to operate as a bridge connection to the WAN; and
- The **Bridge/LLC2 LAN Interface Table** allows you to configure a LAN interface to operate as a bridge connection to the local LAN.

These windows and their functions are described in the following sections.

## Configuring Frame Relay Bridge Ports

You can use the Bridge/LLC2 Frame Relay Interface Table to configure a frame relay port to operate as a bridge connection to the WAN. To access the table:

1. Click on **Device**  to display the Device menu.
2. Drag down to **Bridge/LLC2 Frame Relay Table**, and release. The Bridge/LLC2 Frame Relay Interface Table, [Figure 11-2](#), will appear.



IF #	RLP	Port	DLCI	Priority	BAG	Format	Session Type	Host MAC Address	LAN ID
4	0	2	18	0	0	Native LLC2	Originated	40:00:00:00:00:18	
1	0	2	70	0	0	Native LLC2	Originated	40:00:00:00:00:70	
3	0	2	85	0	0	Native LLC2	Terminated	40:00:00:00:00:85	
5	0	2	86	0	0	Native LLC2	Terminated	40:00:00:00:00:86	
2	0	5	18	0	0	Native LLC2	Originated	40:00:00:00:18:18	

Interface Number : 4      Format : Native LLC2  
 RLP (0-7) : 0      Session Type : Originated  
 Port (0-7) : 2      Host MAC Address :  
 DLCI (16-991) : 18      LAN ID (0-4095) :  
 Priority (0-9) : 0      Blocked Flag : No  
 Bandwidth Allocation Group (1-16) : 0

Add    Modify    Delete  
 Refresh    Close

Figure 11-2. Bridge/LLC2 Frame Relay Interface Table

You can configure the following bridge port parameters (except Interface Number):

**Interface Number**

This is a sequential number used to identify the interface; it will be assigned automatically.

**RLP**

This parameter identifies the RLP containing the frame relay bridge port. Enter 0 for FRX4000 and SmartSwitch 1800 devices (for RLP0); enter 0 - 7 for an FRX6000.

**Port**

This parameter identifies the physical port on the RLP containing the bridge port. Make sure the physical frame relay port is not reserved for backup DLCIs as determined by the Backup Use Only parameter in the Frame Relay Port Configuration window (see Chapter 5, **Frame Relay Status and Configuration**).

**DLCI**

This parameter is a number that identifies a virtual connection in the frame relay network and is usually assigned by the frame relay provider. Make sure the DLCI you select is not part of a frame relay DLCI backup group as determined by the Backup Group Number parameter in the Frame Relay DLCI Table. (See Chapter 5, **Frame Relay Status and Configuration**.)

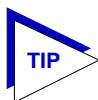
Also, make sure that the DLCI is different than the one configured for the physical port in the frame relay PVC record (see your FRX or SmartSwitch 1800 hardware documentation for more information on configuring frame relay PVC connections).



*Do not configure more than one bridge port per DLCI.*

**Priority**

This field prioritizes the bridge port for traffic within the device; the higher the number, the higher the priority. This priority has no effect on traffic exiting the device. Priorities are configured on all logical interfaces that use a physical frame relay port. The FRX or SmartSwitch 1800 processor uses these priorities to help determine the order in which it will process protocols. The default value for this parameter is 0.

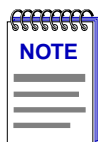


*When configuring priorities, be sure to consider the types of traffic being routed on other connections in the node.*

### Bandwidth Allocation Group

This parameter assigns the bridge port to one of 16 Bandwidth Allocation Groups (BAG).

BAGs regulate bandwidth usage by outgoing traffic on the physical link and can ensure that response time-sensitive traffic get access to the available frame relay bandwidth. Up to 16 groups can be configured through console management (refer to your FRX or SmartSwitch 1800 hardware documentation for more information).



*Bandwidth allocation groups cannot currently be configured via SPMA; for more information on configuring these groups, see your FRX or SmartSwitch 1800 hardware documentation.*

### Format

This field specifies the RFC 1490 encapsulation method that will be used for bridged traffic. Selecting Tb 8023 will add an Ethernet header to the frame; selecting Srb 8025 will add a Token Ring header to the frame; selecting Native LLC2 results in no MAC address header being added to the frame. If Native LLC2 is selected, the interface can only be used for terminated LLC2 traffic. The default value for this parameter is LLC2.

### Session Type

This field is configurable only if you have selected Native LLC2 as your RFC 1490 encapsulation method in the **Format** field (see above). For Session Type, if you select Originated, then LLC2 connections *from* the configured Host MAC Address (see below) can use this interface. If you select Terminated, then connections *to* the configured Host MAC address can use this interface. The default value for this parameter is Originated.

### Host MAC Address

This field is configurable only if you have selected Native LLC2 as your RFC 1490 encapsulation method in the **Format** field (see above). Enter the MAC address of the LLC2 host or workstation to which the remote LAN device needs to connect. This MAC address will match the address of the LLC2 host in the SNA/LLC2 Host Table (see Chapter 7 SNA Status and Configuration, for more information on configuring LLC2 hosts).

### LAN ID

This field is configurable only if you have selected Srb 8025 (Token Ring) as your RFC 1490 encapsulation method in the **Format** field (see above). This ID is only used in an 802.5 Source Route environment and is normally assigned by a system administrator. It identifies the ring number used by the frame relay-compliant source route bridge at the other end of the frame relay PVC.

Each LAN ID must be unique among all LAN IDs throughout the network on which this device will operate.



**Blocked Flag**

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or rebooted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed. The default value for this parameter is **No**.

**Adding or Modifying Frame Relay Bridge Ports**

First, access the Bridge/LLC2 Frame Relay Interface Table (see [Configuring Frame Relay Bridge Ports](#), page 11-4).

To add a new Frame Relay bridge port:

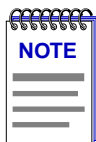
1. Enter the **RLP**, **Port**, and **DLCI** numbers, and the other configurable values for each bridge port.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the Frame Relay Interface you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you make some changes, and would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the Frame Relay Interface you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring a Bridge Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

**Configuring LAN Bridge Ports**

You can use the Bridge/LLC2 LAN Interface Table to configure a LAN interface to operate as a bridge connection to the local LAN. To access the table:

1. Click on  to display the Device menu.

2. Drag down to **Bridge/LLC2 LAN Interface Table**, and release. The Bridge/LLC2 LAN Interface Table, [Figure 11-3](#), will appear.

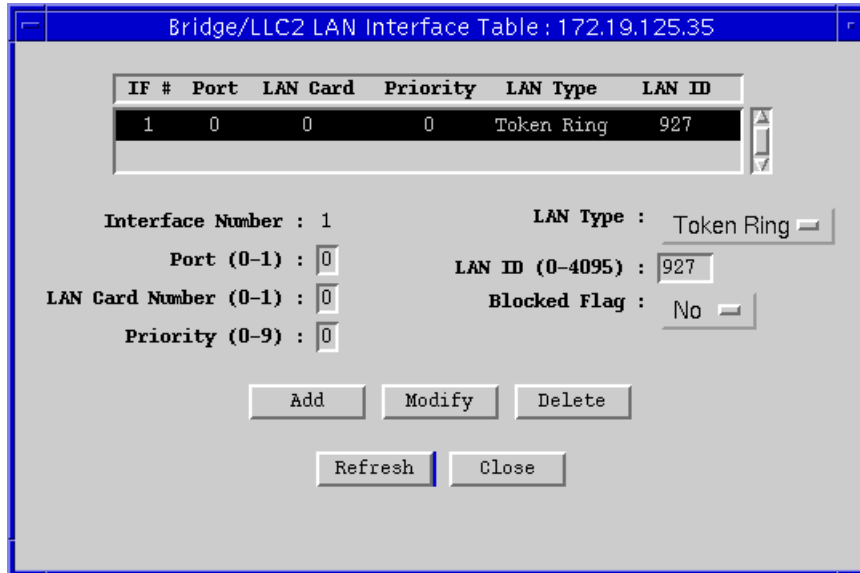


Figure 11-3. Bridge/LLC2 LAN Interface Table

You can configure the following bridge port parameters (except Interface Number):

**Interface Number**

This is a sequential number used to identify the interface; it will be assigned automatically.

**Port**

This field corresponds to the LAN Card Number. Enter 0 for an FRX4000 or SmartSwitch 1800 (for RLP0); enter 0 or 1 for an FRX6000. This number must be identical to the number entered in the **LAN Card Number** field (see below).

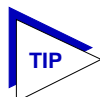
**LAN Card Number**

This field specifies the LAN Card being configured as a bridge port. Enter 0 for an FRX4000 or SmartSwitch 1800 (for RLP0); enter 0 or 1 for an FRX6000. This number must be identical to the number entered in the **Port** field (see above).

**Priority**

This field prioritizes the interface for traffic within the device; the higher the number, the higher the priority. This priority has no effect on traffic exiting the device. Priorities are configured on all logical interfaces that use a physical frame

relay port. The FRX or SmartSwitch 1800 processor uses these priorities to help determine the order in which it will process protocols. The default value for this parameter is 0.



*When configuring priorities, be sure to consider the types of traffic being routed on other connections in the node.*

### LAN Type

This field specifies the LAN type for the LAN card you are configuring as a bridge port. Select Ethernet or Token Ring.

### LAN ID

This field is configurable only if you have selected Srb 8025 (Token Ring) as your RFC 1490 encapsulation method in the **Format** field (see above). This ID is only used in an 802.5 Source Route environment and is normally assigned by a system administrator. It identifies the Token Ring adapter to the network.

Each LAN ID must be unique among all LAN IDs throughout the network on which this device will operate.

### Blocked Flag

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or rebooted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed. The default value is **No**.

## Adding or Modifying LAN Bridge Ports

First, access the Bridge/LLC2 LAN Interface Table (see [Configuring LAN Bridge Ports](#), page 11-7).


To add a new LAN bridge port:

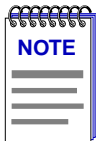
1. Enter the **Port** and **LAN Card** numbers, and the other configurable values for each bridge port.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the LAN Interface you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you make some changes, and would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the LAN Interface you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring a Bridge Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

# SmartSwitch 1800 Voice Configuration

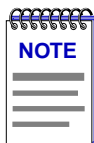
*About SmartSwitch 1800 voice support; configuring system-level voice parameters; speed-dial configuration; configuring voice ports and voice interfaces; viewing voice statistics*

---

The two voice ports in the SmartSwitch 1800 provide connectivity over frame relay for telephones, PBXs (Private Branch Exchange), fax machines, and analog modems.

Calls are routed between voice ports and frame relay ports by internal mapping (using a dial table) that reads the destination node number for a voice call and associates it with a voice interface. The voice interface record includes an associated frame relay port and DLCI over which the Call Request frame will be sent to the destination node.

The SmartSwitch 1800 can combine voice and data frames over the same frame relay DLCI. With the current version of firmware, splitting the voice and data at the other end requires a connection to another Cabletron frame relay device (FRX or SmartSwitch 1800). That device must be configured with a PVC between the network frame relay port and the frame relay port that will transmit only the voice frames. (Once the data and voice frames have been separated in the Cabletron frame relay device, each data frame will be routed based on the DLCI configuration and data type.)



*At the time of this SPMA release, the SmartSwitch 1800 supports the collection of voice port statistics, but does not allow the actual configuration of voice ports or voice interfaces. Full voice support will be included in a future release of SPMA.*

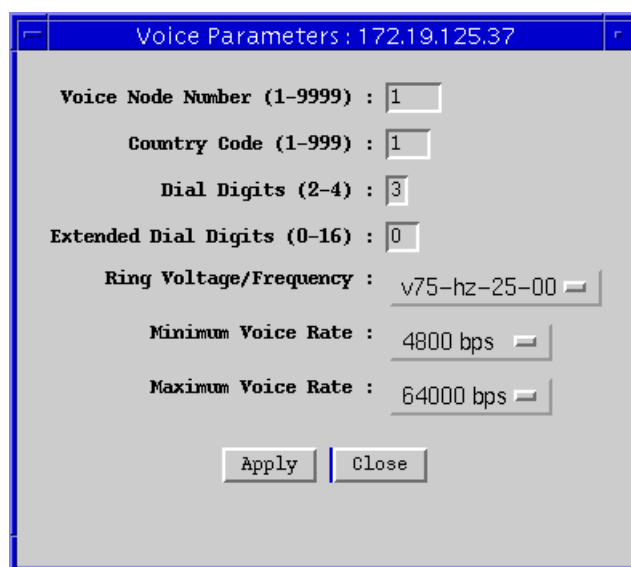
*You can configure voice ports and voice interfaces through console management. Refer to your SmartSwitch 1800 hardware documentation for more information.*

## Configuring System-Level Voice Parameters

Certain voice parameters apply to specific voice ports or interfaces. Others are system level, and apply to all voice calls on the node.

Using the Voice Parameters window, you can configure the system-level voice parameters. To access the window:

1. Click on **Device** to display the Device menu.
2. Drag down to **Voice System Parameters**, and release. The Voice Parameters window, [Figure 12-1](#), will appear.



Voice Parameters : 172.19.125.37

Voice Node Number (1-9999) : 1

Country Code (1-999) : 1

Dial Digits (2-4) : 3

Extended Dial Digits (0-16) : 0

Ring Voltage/Frequency : v75-hz-25-00

Minimum Voice Rate : 4800 bps

Maximum Voice Rate : 64000 bps

Apply Close

Figure 12-1. Voice Parameters

You can configure the following system-level voice parameters:

### Voice Node Number

This number identifies the SmartSwitch 1800 as the source or destination node in call setup frames. This number must be the first four digits of each long-dial number, and is the number that must be dialed to reach a remote device. If a speed-dial number is configured for the long-dial number, the operator can enter that speed-dial number, and the firmware will read the long-dial number from the speed-dial map table.

### Country Code

This code is a telephone prefix code that identifies the country in which the SmartSwitch is installed. The following table contains a list of country codes.

Table 12-1. International Dialing Country Codes

Country	Code	Country	Code	Country	Code
Algeria	213	Indonesia	62	Portugal	351
Argentina	54	Iran	98	Qatar	974
Australia	61	Iraq	964	Romania	40
Austria	43	Ireland	353	San Marino	39
Belgium	32	Israel	972	Saudi Arabia	966
Bolivia	591	Italy	39	Scotland	44
Brazil	55	Japan	81	Senegal	221
Bulgaria	359	Jordan	962	Singapore	65
Chile	56	Kenya	254	South Africa	27
China	86	Korea	82	Spain	34
Colombia	57	Kuwait	965	Sri Lanka	94
Costa Rica	506	Libya	218	Suriname	597
Cyprus	357	Liechtenstein	41	Sweden	46
Czechoslovakia	42	Luxembourg	352	Switzerland	41
Denmark	45	Macao	853	Tahiti	689
Ecuador	593	Malaysia	60	Taiwan	886
Egypt	20	Malta	356	Tanzania	255
El Salvador	503	Mexico	52	Tasmania	61
Ethiopia	51	Monaco	33	Thailand	66
Fiji	679	Morocco	212	Tunisia	216
Finland	358	Netherlands	31	Turkey	90
France	33	Netherl. Antilles	599	Uganda	256
French Antilles	596	New Zealand	64	U.A.E.	971
Gabon	241	Nicaragua	505	United Kingdom	44
Germany	37	Nigeria	234	United States	01
Greece	30	Northern Ireland	44	Uruguay	598
Guam	671	Norway	47	Vatican City	39
Guantanamo Bay	53	Pakistan	92	Venezuela	58
Guatemala	502	Panama	507	Wales	44
Guyana	592	Paraguay	595	Yugoslavia	38

Table 12-1. International Dialing Country Codes

Country	Code	Country	Code	Country	Code
Haiti	509	Peru	51	Zaire, Rep.	243
Honduras	504	Philippines	63	Zambia	260
Hong Kong	852	Poland	48	Zimbabwe	263
India	91				

**Dial Digits**

This field specifies the number of digits used for speed-dial and auto-dial numbers. A speed-dial number is a short substitute for a longer number, and an auto-dial number will be dialed automatically when the receiver is taken off-hook. The default value for this parameter is 3.

**Extended Dial Digits**

This specifies the number of extended dial digits that must be entered by the user of attached equipment as part of a dial string when **Ext. Digits Source** in the Voice Configuration window is set to User (see [Configuring Voice Ports, page 12-8](#)).

Speed-dial numbers and extended digits can be output by remote voice/fax ports.

Extended digits will be forwarded to the remote end of the frame relay connection if all of these conditions are met:

- Extended dial digits are configured in the speed-dial map;
- The parameter **Forwarded Digits** in the Voice Configuration window (see [Configuring Voice Ports, page 12-8](#)) is set to All or Extended;
- The parameter **Ext. Digits Source** in the Voice Configuration window is set to Map.

If the first two conditions are met, but **Ext. Digits Source** is set to User, the operator must enter the extended dial digits to be forwarded.

Setting the number of Extended Dial Digits to a value greater than zero reduces the number of allowable entries in the Voice Speed Dial Configuration window. When the Extended Dial Digits is 0, up to 512 Speed Dial entries can be defined. When Extended Dial Digits is greater than 0, only 256 entries can be defined. The default value for this parameter is 0.

**Ring Voltage/Frequency**

This parameter specifies the voltage and frequency of the telephone ring circuit. In two-wire OPX/FXS mode, the SmartSwitch 1800 provides ring voltage to the telephone when it is called by a remote unit. The frequency of ringing voltage is variable and is a divide by 1, 2, or 3 of the main AC line frequency. The default value for this parameter is v80-hz-20-00.



**Minimum Voice Rate**

This field specifies the minimum operating rate (in bits per second) of all voice channels when congestion occurs. The default value for this parameter is 4800 bps.

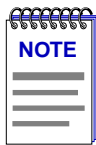
**Maximum Voice Rate**

This field specifies the maximum operating digitization rate (in bits per second) of all voice channels. The default value for this parameter is 64000 bps.

## Changing Parameter Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.
3. Click on  to save your changes.



*After you have made system-level changes (such as configuring voice parameters), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Speed Dial Configuration

The Voice Speed Dial Configuration window contains the dial numbers (similar to telephone numbers) that can be used to call remote devices. The table associates each of these numbers (called long-dial numbers) with a shorter (usually) speed-dial number that can be used to call the device, as well as any configured extended-dial digits that will be forwarded by the device.

To access the window:

1. Click on  to display the Device menu.
2. Drag down to **Voice Speed Dial Configuration**, and release. The Voice Speed Dial Configuration window, [Figure 12-2](#), will appear.

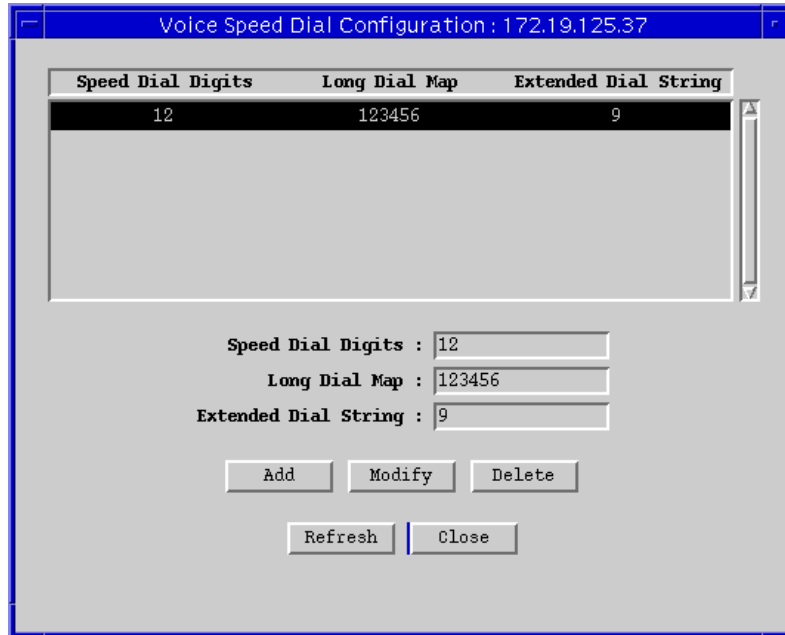


Figure 12-2. Voice Speed Dial Configuration Window

The top part of the window displays a list of configured speed-dial numbers with associated long-dial and extended-dial strings. The bottom part of the window allows you to modify or add the following parameters:

#### Speed Dial Digits

This is the number of characters (1-4) configured for **Dial Digits** in the Voice Parameters window (see [Configuring System-Level Voice Parameters, page 12-2](#)). A question-mark wildcard can be used for any single digit, and an asterisk wildcard can be used for any number of digits.

#### Long Dial Map

This is a six-digit number for which the speed-dial number is a shortcut. The number must identify its associated device as follows.

#### SmartSwitch 1800:

Digits 1-4 = **Voice Node Number**, 0001-9999, configured in the Voice Parameters window (see [Configuring System-Level Voice Parameters, page 12-2](#)).

Digit 5 = 0 or 1. This digit is irrelevant on the SmartSwitch 1800, so either value can be used.

Digit 6 = Channel number 4 or 5, which identifies the Voice Port. (Refer to Chapter 2, [Using the FRX4000, FRX6000, and SmartSwitch 1800 Hub View](#) for information on Voice Port numbers.)

Valid values for the voice concentrator vary depending on the device type; the numbers below relate to ACT Networks' SDM network access devices.

**SDM:**

Digits 1-2= Switch number 01-61.

Digits 3-4= Port number 00-15.

Digit 5= Slot number 1-8 if FP or DX. Slot number 1-4 if JFP.

Digit 6= Channel number 0-5 if DVC. Arbitrary (typically 1-6) if FP or JFP.

**Extended Dial String**

This is an extended set of digits that will be forwarded with the call if **Ext. Digits Source** is set to Map in the Voice Configuration window (see [Configuring Voice Ports, page 12-8](#)). If **Ext. Digits Source** is set to User, any extended digits must be entered by the operator at the initiating device.

Calls placed to a speed-dial number will go to the device (e.g., PBX) whose full number is associated with that speed-dial number in the Voice Speed Dial Configuration window. If extended dial digits are included in the table or the call, the call will automatically be forwarded through the remote device to the telephone number that matches the extended digits.

## Adding or Modifying Speed Dial Numbers

First, access the Voice Speed Dial Configuration Window (see [Speed Dial Configuration, page 12-5](#)).

To add a new Speed Dial Number:

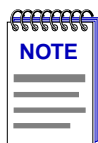
1. Enter the configurable values for each number.
2. Click on  to add your new entry.

To modify an existing entry:

1. In the list box, click to select the number you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)
2. Edit the fields, as desired. If you make some changes, and would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

1. In the list box, click to select the number you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



After you have made system-level changes (such as configuring Voice Parameters, you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.

## Configuring Voice Ports

You can use the Voice Configuration window to configure a voice port. To access the window:

1. Click mouse button 3 on the voice port of interest to display the Port Menu.
2. Drag down to **Voice Configuration**, and release. The Voice Configuration window, [Figure 12-3](#), will appear.

Voice Configuration RLP 0 Port 4					
DTMF (0-255) :	<input type="text" value="30"/>	Num Digits Delete (0-4) :	<input type="text" value="0"/>	Speed :	<input type="text" value="8000 bps"/>
TE Timer (0-255) :	<input type="text" value="3"/>	Forward Delay (0-40) :	<input type="text" value="2"/>	Interface :	<input type="text" value="Loop Start"/>
Call Timer (1-30) :	<input type="text" value="5"/>	Make Ratio (20-80) :	<input type="text" value="34"/>	Telephony Type :	<input type="text" value="OPX"/>
Dial Timer (0-10) :	<input type="text" value="0"/>	Break Ratio (20-80) :	<input type="text" value="66"/>	Hunt Group :	<input type="text" value="A"/>
SLT Timeout (1-99) :	<input type="text" value="30"/>	DTMF On Duration (30-1000) :	<input type="text" value="100"/>	Suppression :	<input type="text" value="High"/>
Jitter (10-255) :	<input type="text" value="165"/>	DTMF Off Duration (30-1000) :	<input type="text" value="100"/>	Ext. Digits Source :	<input type="text" value="Map"/>
Sample Delay (0-255) :	<input type="text" value="0"/>	Auto Dial :	<input type="text" value="Enabled"/>	Forwarded Type :	<input type="text" value="DTMF"/>
Level In (-22 to 7) :	<input type="text" value="0"/>	Auto Dial Number :	<input type="text" value=""/>	Forwarded Digits :	<input type="text" value="None"/>
Level Out (-22 to 7) :	<input type="text" value="0"/>	Auto Poll :	<input type="text" value="Enabled"/>	Tone Type :	<input type="text" value="DTMF"/>
Long Dial Prefix :	<input type="text" value="0"/>	Auto Poll Timer (5-30) :	<input type="text" value="10"/>	Blocked Flag :	<input type="text" value="Disabled"/>
				Link Down Busy :	<input type="text" value="Enabled"/>
				Fax Supported :	<input type="text" value="Yes"/>
<input type="button" value="Apply"/> <input type="button" value="Close"/>					

Figure 12-3. Voice Configuration

You can configure the following voice port parameters:

### DTMF

This parameter enables, disables, or specifies a time span over which Dual Tone Multi Frequency (DTMF) tones will be regenerated. (DTMF tones are the “beeps” usually heard when dialing a touch-tone telephone.) Enter 0 to disable DTMF: the

DTMF tones are passed transparently to the remote device. Enter 1 to enable DTMF: the SmartSwitch will detect incoming tones and regenerate them as received. Enter 2-255 to specify a number of seconds the SmartSwitch will regenerate DTMF tones (including call setup). The default value for this parameter is 1, enable DTMF.

#### TE Timer

The Timed E Timer parameter is relevant only if **Interface** (see below) is EM. It is the time (in seconds) of the delay after which the EM “E” lead follows the “M” lead. The default value for this parameter is 3.

#### Call Timer

This field is the amount of time (in seconds) the SmartSwitch 1800 will wait for a response to a Call Connect or a Call Clear request. When the SmartSwitch issues the Call Connect or Call Clear request, it will set a timer to the value configured here. If that timer expires with no response from the destination, the SmartSwitch will generate a busy tone. The default value for this parameter is 5.

#### Dial Timer

This is the delay (in seconds) the SmartSwitch 1800 will use to determine when variable-length dialing is complete. (Variable-length dialing allows the user to place a call without entering the configured number of digits for the speed dial number.)

When the operator of the attached voice/fax equipment dials a digit that is not the configured **Long Dial Prefix** (see below), the SmartSwitch 1800 assumes a speed-dial number is being dialed and activates the Dial Timer. If the timer expires with no new digit entries, the SmartSwitch will assume dialing is complete.

The default value for this parameter is 0. A setting of 0 means the Dial Timer will never expire. The SmartSwitch 1800 will wait indefinitely for the operator to enter the digits.

If the number of dialed digits is less than the value specified for **Dial Digits** in the Voice Parameters window (see [Configuring System-Level Voice Parameters, page 12-2](#)), the SmartSwitch will “pad” the dialed number with leading zeros before searching the speed-dial configuration map. For example, assume **Dial Digits** is 4 and the user has dialed 33 when the Dial Timer expires. The speed dial number 0033 will be used to search the speed-dial map for a defined destination.

Note that regardless of the Dial Timer setting, any of the following conditions and/or configurations will disable variable-length dialing:

- Long-call-format dialing is being used. The SmartSwitch 1800 assumes this format is being used if the first digit dialed is the character configured for **Long Dial Prefix** (see below);
- The **Num Digits Delete** parameter (see below) is set to any value greater than 0;
- **Auto Dial** (see below) is set to Enabled.

### **SLT Timeout**

This is the time (in seconds) the local voice port will wait before an actual fax transmission begins. If there is no fax tone when this timer expires, the connection will be terminated. The default value for this parameter is 30.

### **Jitter**

This field specifies the amount of jitter delay (in 5-millisecond increments), which is used to compensate for the variable arrival time of frames. Inconsistent arrival can result in a choppy voice quality. Increasing the jitter buffer size will increase the end-to-end delay, but will insure smoother voice quality.

### **Sample Delay**

This field specifies the amount of sample delay.

### **Level In**

This specifies the local voice level into the voice port. This parameter adjusts the sensitivity of the local voice channel to the signal from the attached device. The purpose of this parameter is to match the voice channel dB level to the input signal. A more negative setting produces a higher input gain (i.e., 7 produces the least input gain and -22 produces the highest input gain). If the In level is reduced (made more negative), the voice channel will be more sensitive to the input; this will cause the voice output at the remote device to sound louder.

The default value for this parameter is 0.

### **Level Out**

This parameter specifies the local voice level out of the voice port. A more positive setting produces a higher volume (i.e., 7 produces the highest volume, -22 the lowest). The default value for this parameter is -4.

### **Long Dial Prefix**

This parameter specifies a character or number that will be required preceding calls using the long-call format (i.e., when a speed-dial number is not used). When the user at an attached device (e.g., telephone or fax machine) dials a long-form number, the number must be preceded by the Long Dial Prefix. Valid values are the digits 0-9 and the characters \* (asterisk) and # (pound sign). The default value for this parameter is \* (asterisk).

### **Num Digits Delete**

This specifies the number of leading dial digits that will be deleted before a dial string is forwarded. This parameter is primarily used to delete leading digits that may be inserted by an attached PBX. For example, assume the user of attached equipment dials 1234 and the attached PBX inserts the number 9 as a prefix to the dial string. If Num Digits Delete is set to 1, the SmartSwitch 1800 will remove the 9 before forwarding the dialed digits 1234. The default value for this parameter is 0.

### **Forward Delay**

This parameter is relevant only if **Forwarded Digits** (see below) is set to All or Extended. It specifies the time (in 0.25 second increments) for two delays:

- the delay before extended digits are forwarded;
- the length of a pause that can be inserted in an extended dial string that is being forwarded. Each time a comma is encountered in an extended string, the SmartSwitch 1800 will pause for the length of time configured for Forward Delay before additional extended digits are forwarded.

The default value for this parameter is 2 (0.5 seconds).

### **Make Ratio**

This parameter is relevant only if **Forwarded Digits** (see below) is set to All or Extended and **Forwarded Type** (see below) is set to Pulse. It specifies the make ratio of each digit pulse that is forwarded. Make periods are the times contact is made for each digit.

Valid values are 20-80 (in increments of 2); the default value is 34.

### **Break Ratio**

This parameter is relevant only if **Forwarded Digits** (see below) is set to All or Extended and **Forwarded Type** (see below) is set to Pulse. It specifies the break ratio of each digit pulse that is forwarded. Break periods are the times contact is broken between digits.

Valid values are 80-20 (in increments of 2); the default value is 66.

### **DTMF On Duration**

This parameter is relevant only if **Forwarded Digits** (see below) is set to All or Extended and **Forwarded Type** (see below) is set to DTMF. This specifies the length (in milliseconds) of a tone that will be used to produce a single DTMF digit. The default value for this parameter is 100.

### **DTMF Off Duration**

This parameter is relevant only if **Forwarded Digits** (see below) is set to All or Extended and **Forwarded Type** (see below) is set to DTMF. This specifies the length (in milliseconds) of silence between DTMF tones in a dial digit string. The default value for this parameter is 100.

### **Auto Dial**

This parameter enables or disables the auto-dial feature of the SmartSwitch 1800. If auto-dialing is enabled, the SmartSwitch will dial the configured **Auto Dial Number** (see below) when the handset attached to this voice port is taken off-hook. The default value for this parameter is Disabled. Enabling this parameter will disable the variable length dialing feature for this channel, regardless of the **Dial Timer** setting (see above).

### Auto Dial Number

This parameter is only configurable if **Auto Dial** (see above) is Enabled. It is a number to which the SmartSwitch 1800 will attempt to connect when the handset (or its equivalent) attached to this port is taken off-hook. The SmartSwitch will automatically dial the long-form number defined in the Speed Dial Configuration table that is associated with the speed dial number specified here.

The number of digits you can enter is determined by the **Dial Digits** parameter configured in the Voice Parameters window (see [Configuring System-Level Voice Parameters](#), page 12-2).

### Auto Poll

This parameter is only relevant if **Auto Dial** (see above) is Enabled. When Auto Poll is enabled, the SmartSwitch 1800 polls the destination device with the frequency specified by **Auto Poll Timer** (see below). If the poll is not acknowledged, the SmartSwitch will “busy out” the channel.

This parameter can be useful in situations where the destination is an emergency number that must always be available. If the destination does not answer the automatic poll, the busy-out condition will notify an attached PBX that the emergency call should be routed to another call routing device.

The default value for this parameter is Disabled.

### Auto Poll Timer

This parameter is only configurable if **Auto Poll** (see above) is Enabled. It is the frequency (in seconds) with which an Auto Poll will be sent. The default value for this parameter is 10.

### Speed

This specifies the speed of the port and is transmitted as part of a Call Setup frame. A voice call will be established if there is enough bandwidth at each end to provide the minimum configured rate. The default value for this parameter is 8000 bps.

### Interface

This parameter, in conjunction with the **Telephony Type** parameter (see below) specifies the type of interface that will be used by the voice channel.

Telephony Interface Type	Interface
OPX (FXO)	Loop Start
SLT (FXS)	Loop Start
EM	4W EM, 4W EM TE, 2W EM, 2W EM TE
AC 15	AC 15A or AC 15C

Loop Start and OPX operating modes provide characteristics similar to those of a central office. Loop Start and SLT operating modes provide characteristics similar to those of a standard telephone set.

EM is an interface used for PBX tie-trunk connections. When EM is specified, the SmartSwitch 1800 acts like the trunk side of a PBX.



4W EM is the normal setting for a PBX EM tie-line interface that uses one pair of wires for the incoming voice signal and another pair of wires for the outgoing voice signal. 2W EM is for an EM tie line that uses a single pair of wires for both the incoming and outgoing voice signal.

AC 15A or AC 15C are 4-wire signaling systems used by PBXs to communicate with each other and other PBX-like communications equipment.

2W EM and 4W EM can be configured in these modes, via the switches on the front of the SmartSwitch:

- 2W EM or 4W EM IS (Immediate Start), the industry standards for EM operation;
- 2W EM or 4W EM DD (Delay Dial), which will cause the SmartSwitch to expect an attached PBX to raise its M-lead to request a dial register. The SmartSwitch will respond as follows: 1) toggle the E-lead, 2) send a dial register to the PBX, 3) return the E-lead to its original state, and 4) wait for dial digits from the PBX (no dial tone is transmitted to the PBX).
- 2W EM or 4W EM WS (Wink Start), which will cause the SmartSwitch to expect an attached PBX to raise its M-lead to request a dial register. The SmartSwitch will respond by sending a dial register to the PBX. When the PBX indicates it is ready for dial digits (no dial tone is transmitted to the PBX), the SmartSwitch will toggle the E-lead. When the E-lead returns to its original state, the PBX will transmit dial digits to the SmartSwitch.

If 2W EM TE or 4W EM TE (Timed EM) is selected, you can specify a delay time for when the E-Lead follows the M-Lead in the **TE Timer** parameter (see above).

The default value for this parameter is Loop Start.

### Telephony Type

This parameter, in conjunction with the **Interface** parameter (see above) specifies the type of interface that will be used by the voice channel. Refer to your SmartSwitch 1800 hardware documentation for more information about selecting the appropriate interface. If EM is specified, you must also set Switch 2 on the front of the SmartSwitch to select an EM type. Refer to your hardware documentation for more information on EM Switch Settings.

The default value for this parameter is OPX.

### Hunt Group

This parameter is not currently supported and must be set to None.

### Suppression

This parameter specifies a level of suppression of background noise. For most calls, low suppression should be sufficient. The higher the suppression level, the greater the possibility that low-volume voice will be lost; therefore, suppression levels higher than low should be used only if it can be certain that background noise will be low or all of the voice transmitted will be sufficiently louder than the background noise.

A higher suppression level saves composite bandwidth, allowing more data channels to operate simultaneously with voice channels. The default value for this parameter is low.

#### **Ext. Digits Source**

This parameter is relevant if the **Dial Digits** parameter configured in the Voice Parameters window (see [Configuring System-Level Voice Parameters, page 12-2](#)) is greater than 0. It specifies the source of extended digits when the user of attached equipment dials a speed-dial number. When Map is specified, extended digits are taken from the **Extended Dial String** in the Speed Dial Configuration Table. When User is specified, extended digits are taken from the user of attached equipment (i.e., the user must dial a speed-dial number and an extended digit string).

If you specify User, you must set the **Dial Timer** (see above) to a value other than 0. The default value for this parameter is Map.

#### **Forwarded Type**

This parameter is relevant only if **Forwarded Digits** (see below) is set to All or Extended. It specifies how the dial digits will be forwarded. The default value for this parameter is DTMF (dual-tone).

#### **Forwarded Digits**

This parameter specifies which dial digits (if any) to forward (i.e., to output at the remote voice / fax card). If None is selected, dial digits are not forwarded to the destination device when a call is initiated on this port. If All is selected, the speed-dial number and associated extended digits are forwarded to the destination device. If Extended is selected, only the extended digit string is forwarded. The source of extended digits (i.e., from the map table or dialed by the user) is specified by **Ext. Digits Source** (see above). The default value for this parameter is None.

#### **Tone Type**

This parameter determines whether the multi-frequency tone will be DTMF (dual-tone) or MF (single-tone). The default value for this parameter is DTMF.

#### **Blocked Flag**

This value will cause the port to be enabled (if **No**) or disabled (if **Yes**) when the device is powered up or rebooted. Whichever state is selected, the port will remain in that state until this value is changed or until an enable or disable action is performed. The default value is **No**.

#### **Link Down Busy**

This parameter enables or disables automatic busy-out of channels when the link is down. When this parameter is enabled, the system will automatically busy-out channels when the composite link is down. When disabled, channels remain on-hook when the link is down. If your application is connected to a PBX that can route calls to an alternate source (e.g., an ACD) based on an “all busy” condition, enable this parameter so the PBX will recognize this condition and reroute the

calls while the composite link is down. This parameter affects on-hook channels only when the link-down condition occurs. Active calls remain in progress until they return to on-hook. The default value for this parameter is Enabled.

### Fax Supported

This specifies whether or not faxes will be transmitted on the port. If **No** is selected, all calls will be treated as voice. If **Yes** is selected, both voice and fax will be transmitted. In most cases, this parameter should be enabled, to allow both voice and fax calls to be processed. The default value for this parameter is **Yes**.

If a voice call experiences excessive noise while this parameter is enabled, the SmartSwitch 1800 might interpret it as a fax call. Disabling this parameter will cause the call to be treated as voice regardless of noise conditions.

## Changing Port Configuration Values

You can edit the values in any field which provides a text box or menu button selection; to do so:

1. To edit a text field, remove the existing value and enter the new value.
2. To edit a field with a menu button, click on the button to display a list of options, then drag down to select the option you want.
3. Click on  to save your changes.

## Applying Port-level Changes

After you have made any port-level configuration changes, your changes will not take effect until you have done an on-line update. To do so:

1. Click mouse button 3 on the port you have been configuring to display the Port Menu.
2. Drag down to **On-line Update** and release.

## Configuring Voice Interfaces

Voice *ports* connect the SmartSwitch 1800 to telephony equipment. Connections to the frame relay network are made over Voice *Interfaces*, which are assigned to DLCIs on physical frame relay ports.

A Voice Interface configuration contains node numbers that identify the local SmartSwitch 1800 and the device at the remote end of the frame relay connection. When a call is received, the dialing scheme in the SmartSwitch 1800 checks the node number addressed in the call against a list maintained by the firmware. If the number is that of the remote node (called the “peer” node), the call is forwarded out the frame relay port.

You can configure a Voice Interface using the Voice Interface Config window. To access the window:

1. Click on **Device** to display the Device menu.
2. Drag down to **Voice Interface Configuration**, and release. The Voice Interface Config window, [Figure 12-4](#), will appear.

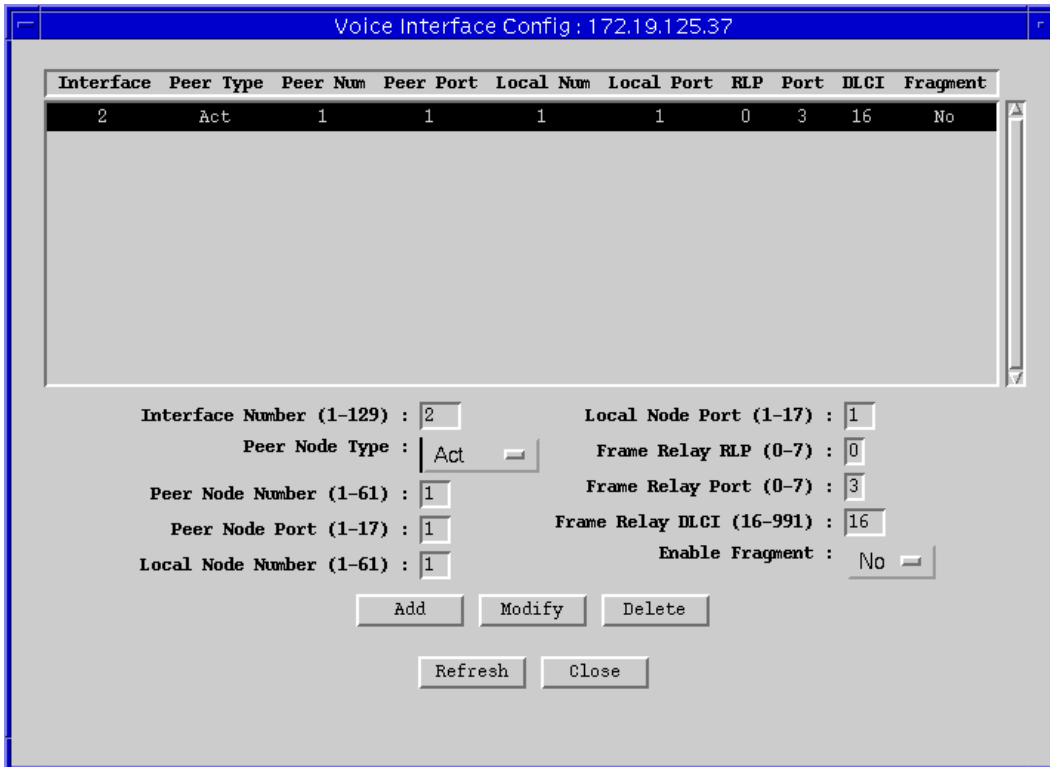


Figure 12-4. Voice Interface Config

You can configure the following parameters for each Voice Interface:

**Interface Number**

In this field enter a number 1 to 129. This is merely a sequential number used to identify the interface.

**Peer Node Type**

This parameter specifies whether the node at the remote end of the frame relay connection is a SmartSwitch 1800 (select Netlink) or a voice concentrator (select ACT).

**Peer Node Number**

This parameter is not used if the peer node type is a SmartSwitch 1800. Enter a number 1 to 61 to specify the node number of the remote device.

**Peer Node Port**

This parameter is not used if the peer node type is a SmartSwitch 1800. Enter a number 1 to 17 to specify the voice port number on the remote device.

**Local Node Number**

This parameter is not used if the peer node type is a SmartSwitch 1800. Enter a number 1 to 61 to specify the node number of the local SmartSwitch 1800. This number must match the **Voice Node Number** entered in the system-level Voice Parameters window (see [Configuring System-Level Voice Parameters](#), page 12-2). The default value for this parameter is 1.

**Local Node Port**

This parameter is not used if the peer node is a SmartSwitch 1800. Enter a number 1 to 17 to specify the voice port number on the local SmartSwitch 1800.

**Frame Relay RLP**

Enter the RLP number of the logical interface of this end of the frame relay link. This would always be 0 for RLP0 on the SmartSwitch 1800.

**Frame Relay Port**

Enter the port number of the local frame relay port over which Voice will be transmitted. This will be port numbers 0 through 3 on the SmartSwitch 1800.

**Frame Relay DLCI**

Enter a number 16 to 991 specifying local frame relay DLCI over which Voice will be transmitted.

**Enable Fragment**

This parameter is not currently supported and must be set to **No**.

## Adding or Modifying Voice Interfaces


First, access the Voice Interface Config Window (see [Configuring Voice Interfaces](#), page 12-15).

To add a new Voice Interface:


1. Enter the configurable values for each interface.
2. Click on  to add your new entry.

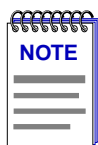
To modify an existing entry:

1. In the list box, click to select the interface you wish to modify. The selected entry will be highlighted. (Note that you can only modify one entry at a time.)

2. Edit the fields, as desired. If you make some changes, and would like to return to the original values, click on the **Refresh** button.
3. Click on  to modify the selected entry.

To delete an existing entry:

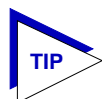
1. In the list box, click to select the interface you wish to delete. The selected entry will be highlighted. (Note that you can only delete one entry at a time.)
2. Click on  to delete the selected entry.



*After you have made system-level changes (such as configuring a Voice Interface), you must apply those changes by rebooting the FRX or SmartSwitch 1800 device, or through console management via the [F7] command.*

## Viewing Voice Statistics

The Voice Statistics window provides general information about voice traffic that is being transmitted across the selected port.



*The statistical windows display their information via the SPMA Meters application; for more information on how to manipulate and configure these meters, see the **SPMA Tools Guide**.*

To access the window:

1. Click mouse button 3 on the voice port of interest to display the Port Menu.
2. Drag down to **Voice Stats**, and release. The Voice Statistics window, [Figure 12-5](#), will appear.

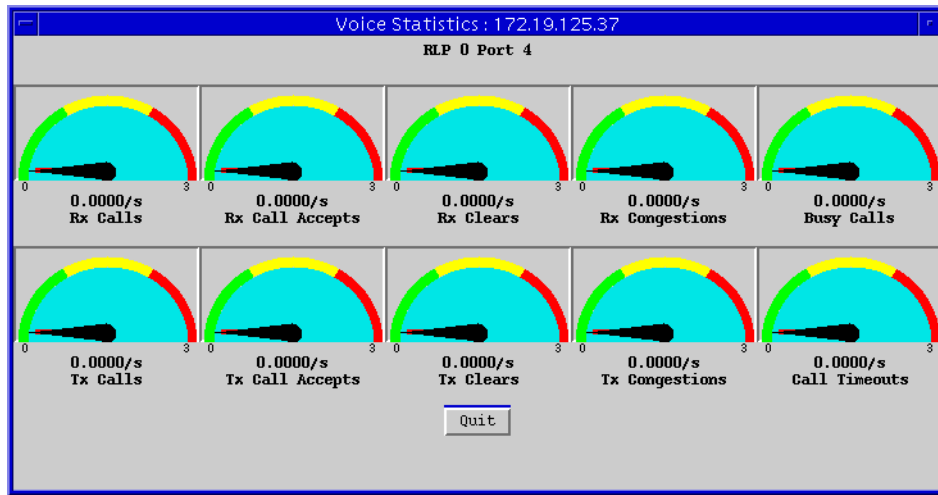


Figure 12-5. Voice Statistics

The Voice Statistics window provides the following statistical data:

**Calls (Received and Transmitted)**

Displays the number of calls that were received or transmitted across the selected port, expressed as a rate (calls/second).

**Call Accepts (Received and Transmitted)**

Displays the number of call accepts that were received or transmitted across the selected port, expressed as a rate (calls/second).

**Clears (Received and Transmitted)**

Displays the number of calls (received or transmitted) that were cleared, expressed as a rate (clears/second).

**Congestions (Received and Transmitted)**

Displays the number of congestion management frames that were received or transmitted across the selected port, expressed as a rate (frames/second).

**Busy Calls**

Displays the number of calls which received a busy indication, expressed as a rate (busy calls/second).

**Call Timeouts**

Displays the number of calls which transmitted time-out to the network, expressed as a rate (call time-outs/second).





# FRX4000, FRX6000, and SmartSwitch 1800 MIB Components

*FRX4000, FRX6000, and SmartSwitch 1800 management information base configuration*

---

## IETF MIB Support

In addition to its proprietary features, the FRX4000, FRX6000, and SmartSwitch 1800 currently support the following IETF MIBs:

- RFC 1213 MIB for Network Management of TCP/IP-based Internets: MIB-II
- RFC 1231 IEEE 802.5 Token Ring MIB (*beginning with firmware version 3.3.1*)
- RFC 1315 MIB for Frame Relay DTEs
- RFC 1381 and RFC 1382 for X.25 (*beginning with firmware version 4.0*)
- RFC 1398 Definitions of Managed Objects for Ethernet-Like Interface Types (*beginning with firmware version 3.3.1*)
- RFC 1490 Multiprotocol Interconnect over Frame Relay
- RFC 1493 Definitions of Managed Objects for Bridges (*beginning with firmware version 3.3.1*)
- RFC 1643 802.3 Ethernet Statistics (*beginning with firmware version 4.0*)
- RFC 1747 Definitions of Managed Objects for SNA Data Link Control (SDLC)
- RFC 1748 802.5 Token Ring Statistics (*beginning with firmware version 4.0*)
- Novell IPX MIB (*beginning with firmware version 3.3.1*)

## **CSI Netlink MIB Support**

In addition to the IETF standard MIBs listed above, the FRX4000, FRX6000, and SmartSwitch 1800 support a number of proprietary features contained in the CSI Netlink MIB. For a copy of this MIB, consult your FRX4000, FRX6000, or SmartSwitch 1800 hardware documentation, or contact Cabletron Systems' Global Call Center.

**A**

Accept Reverse Charge 5-20, 6-7  
 Address 7-8, 7-11, 7-16  
 Address Table 4-6, 4-8  
 Admin Status 2-13  
 Algorithm 4-6  
 algorithm (subscriber table) 4-4, 4-5  
 alternate subscriber addresses 4-6  
 ansiT1 617 D 5-7  
 Answer Non Configured 8-6  
 ANXD 5-21  
 Applying Port-level Changes 2-34, 5-8, 5-20,  
 6-8, 7-7, 7-15, 8-6  
 Auto Call 8-8  
 Auto Call Enabled 7-9  
 Auto Dial 12-11  
 Auto Dial Number 12-12  
 Auto Poll 12-12  
 Auto Poll Timer 12-12

**B**

backup DLCI 5-11  
 Backup Group Number 5-11  
 Backup Groups 5-12  
 Backup Protocol 5-11  
 Backup Use Only 5-7  
 BAG (Bandwidth Allocation Group) 9-5, 10-4  
 Bandwidth Allocation 5-7  
 Bandwidth Allocation Group 5-17, 7-13, 11-6  
 BECN (backward explicit congestion  
 notification) 5-23  
 BECN Recovery Count 5-10  
 binary synchronous communications  
 (BSC) 8-1  
 Blocked Flag 5-19, 6-6, 8-5, 10-5, 11-7, 11-9,  
 12-14  
 Blocked Port Flag 5-6  
 Break Ratio 12-11  
 Bridge Enabled 11-3  
 Bridging Parameters 11-1  
 bridging support 11-1  
 Broadcast Address 9-6, 9-10

BSCI 8-1  
 BSCI Subscriber Information 8-7

**C**

Call Info in Request Packet 8-4  
 call requests 4-1, 4-5  
 Call Timer 12-9  
 Call User Groups  
     Make Calls Outside CUG 5-19, 6-5  
     Rcv Calls Outside CUG 5-18, 6-5  
 Changes, applying 2-34  
 Charts and Meters 1-4  
 Circuit Index 10-13  
 Clear VC on Last Dev Down 8-6  
 Closed User Group 5-18, 6-4  
 Closed User Group Index 5-18, 6-5  
 Committed Burst Size (BC) 5-10  
 Committed Information Rate (CIR) 5-9  
 community name 2-1, 2-2  
 Configuring IP Interface Secondary  
     Adresse 9-9  
 Configuring IP Interfaces 9-2  
 Configuring IPX Interfaces 10-2  
 Configuring SNA Ports 7-2  
 Connection ID 8-8, 8-10  
 Connection Priority 4-5  
 Connection Without Poll 8-6  
 Connector Type 2-15, 6-5  
 Contact Status 2-7  
 Control Unit ID 8-10  
 Country Code 12-2

**D**

Data Mode 7-17  
 DCE 5-4, 5-5, 5-6, 7-5, 8-5  
 Default Packet Size 5-17, 6-4  
 Default Throughput Class 5-18, 6-4  
 Desired Operational State 7-17  
 Desired State at Startup 7-17  
 Destination Address 9-6  
 Destination Subscriber 9-6, 10-5

- Device Information 2-9
- Device menu 2-9
- Device Unit ID 8-10
- Diagnostics Enabled 10-6
- Dial Digits 12-4
- Dial In/Out 6-6
- Dial Timer 12-9
- Disable Rqst Disconnect 7-6
- discard eligible (DE) 5-10, 5-22
- Disconnect (DISC) 6-9
- Disconnect Mode (DM) 6-9
- Disconnect Timer 6-3
- DLCI 5-9
- DLCI Number 5-16
- DLCI Priority 5-11
- DTE 5-4, 5-5, 5-6, 7-5, 8-5
- DTMF 12-8
- DTMF Off Duration 12-11
- DTMF On Duration 12-11

## E

- EBCDIC character set 8-4
- Encapsulation Method 5-19
- End-to-End ACK 8-5
- Error Retransmit Count 8-4
- Error Threshold 5-4
- Ethernet Frame Type 11-3
- Excess Burst Size (BE) 5-10
- Ext. Digits Source 12-14
- Extended Dial Digits 12-4
- Extended Dial String 12-7

## F

- Fast Select 5-20, 6-7
- Fax Supported 12-15
- FCS Errors 2-26
- FECN (forward explicit congestion notification) 5-23
- firmware versions 1-8, 2-8, A-1
- Flow Control Negotiation 5-19, 6-7
- Format 11-6
- Forward Delay 12-11
- Forwarded Digits 12-14
- Forwarded Type 12-14
- Forwarding Table Size 11-2
- Frame Reject (FRMR) 6-11
- frame rejects 2-27
- frame relay access device 1-1
- Frame Relay Backup Groups 5-12

- Frame Relay Bridge Ports 11-4
- Frame Relay DLCI 12-17
- frame relay operational parameters 5-2
- Frame Relay Port 12-17
- Frame Relay RLP 12-17
- Frame Type 10-4
- Frames Discarded 5-23
- Frames Queued 2-26
- frx 2-1
- FRX firmware versions 1-8
- FRX4000 and FRX6000, descriptions 1-1
- Full Duplex 8-5

## G

- Gateway Address 10-11
- Generate Clock 5-6, 6-6, 7-5, 8-5
- Global Find MAC Address 1-4
- Global TFTP 1-4
- Group Poll Address 7-17

## H

- Health statistics
  - LAN Card 2-27
  - RLP 2-25
  - serial port 2-26
- Help 1-7
- History button 1-5
- Host Index 7-19
- Host MAC Address 11-6
- hostname 2-2
- HPAD 8-6
- HSAP 7-25

## I

- ICMP Add Routes 9-5
- IDBLK 7-12
- Idle Fill Char 7-6
- IDNUM 7-12
- IETF MIBs, supported by FRX devices A-1
- ifIndex 2-15, 2-21
- ifSpeed 2-15
- In Call Bar 5-20, 6-7
- Inactivity Timer 6-3, 7-4
- indexing (RLPs and LAN cards) 2-2
- Information Transfer (INFO) 6-10
- Interface Number 9-3, 10-3, 11-8, 12-16
- Interface Type 10-4
- Interface, Voice Channel 12-12

Intervening Networks 10-11  
 Inverse ARP 9-8  
 IP address 2-8  
 IP Enabled 11-3  
 IP interface 9-2, 10-2  
 IP Interface Type 9-4  
 IP Node Defaults 9-1  
 IPX Enabled 11-3  
 IPX interface 10-1  
 IPX Network Address 10-2  
 IPX Node Defaults 10-1  
 IPX Static Routes 10-10

## J

Jitter 12-10

## L

L1 Duplex 7-6  
 L2 Data Mode 7-9  
 LAN Bridge Ports 11-7  
 LAN Card 9-6, 10-5  
 LAN card displays 2-2  
 LAN card indexing 2-3  
 LAN Card Number 11-8  
 LAN ID 11-6, 11-9  
 LAN Type 11-9  
 LAPB command and response frames 6-8  
 Least LCN 4-4  
 Level In 12-10  
 Level Out 12-10  
 LIC displays 2-3  
 LIC Type 2-18  
 Line Busy 4-4  
 Line Failed 4-4  
 Line Speed 5-3, 7-3, 8-3  
 Link Down Busy 12-14  
 Link Integrity Timer 5-4, 5-5  
 Link Layer Management 5-6  
 Link Station Configuration 7-15  
 Link Station Rx Statistics 7-30  
 Link Station Statistics 7-29  
 Link Station Tx Statistics 7-30  
 linkup 2-13  
 LLC2 Configuration 7-18  
 LLC2 Connection 7-9  
 LLC2 Host Connections 7-24  
 LMI 5-21  
 LMI rev 1 5-7  
 Local MAC Address 7-11

Local Node Number 12-17  
 Local Node Port 12-17  
 Local SAP Address 7-11  
 Local Subscriber ID 7-25, 8-8  
 Local Subscriber Id 7-8  
 Location (on Hub View front panel) 2-7  
 Logical DCE 5-6  
 Logical Port Configuration 5-15  
 logical port indices 4-5  
 Logical Ports 5-1, 5-15, 5-16  
 Logical Rejects 2-27  
 Long Dial Map 12-6  
 Long Dial Prefix 12-10  
 LP 4-5  
 LPDA Resource Id 7-9  
 LPDA Support 7-5

## M

Make Ratio 12-11  
 Max Bytes per Frame 5-3  
 Max Frame Size 8-2  
 Max Packet Size 2-15, 5-17, 6-4  
 Max Retransmissions 8-3  
 MAX Retries 7-4  
 Max RX PDU Size 7-16  
 Max Rx UnACK I-Frames 7-16  
 Max TX PDU Size 7-16  
 Max Tx UnACK I-Frames 7-16  
 Max VC 9-7, 10-9  
 Maximum Supported VCs 5-5  
 Maximum Transmission Unit 9-4, 10-4  
 Maximum UnACK Packets 5-18, 6-4  
 Maximum Voice Rate 12-5  
 Memory 2-17  
 menu structure 2-10  
 meters 2-12, 2-24, 5-2, 5-21, 6-1, 7-2, 7-26, 12-18  
 MIB I, II 1-4, 2-7, 2-9  
 MIBTree 1-4  
 Minimum Voice Rate 12-5  
 module status color codes 2-5  
 Modulus 7-17  
 Monitored Events Count 5-5  
 Multidrop 8-4

## N

N1 Polling Count 5-4, 5-5  
 N2 Error Threshold 5-4  
 N2-Expired T1 LPDUs 7-22  
 N2-Max LPDUs 7-13

N3 Monitored Events Count 5-5  
N3-LPDU Count 7-22  
N3-Max Info LPDUs 7-13  
NAK Retry Count 8-4  
Name 7-16  
Name (on Hub View front panel) 2-7  
NetBIOS Enabled 10-6  
NetBIOS Hops 10-8  
Network Address 10-4, 10-11  
Network Mask 9-4, 9-10  
Network Number 10-13  
Network Trunk Group 6-6  
no LMI 5-6  
No Response Retries 8-3  
No Response Timer 8-3  
Node Address 10-11  
Node Community Name 2-2  
NRZ Data Encoding 7-5  
Num Digits Delete 12-10

## O

On-line Update 2-34  
Operation Status 2-12  
Out Call Bar 5-20, 6-7  
Outgoing Rate Control 5-7, 5-10

## P

Packet Size 7-3  
PAD Type 7-5, 8-6  
Path 4-5  
Peer Node Number 12-17  
Peer Node Port 12-17  
Peer Node Type 12-16  
Periodic RIP Enabled 10-7  
Periodic RIP Timer 10-8  
Periodic SAP Enabled 10-6  
Periodic SAP Timer 10-8  
Permanent Virtual Circuits (PVCs) 4-1  
physical port indices 4-5  
Physical Port Interface 5-5, 7-4, 8-5  
Polling Count 5-4, 5-5  
Polling Intervals 2-9, 2-32  
Polling Verification Timer 5-5  
port display forms 2-12  
Port State 2-13  
port status color codes 2-5  
Port Type 2-13  
Port-level Changes 5-8  
Prevent Local Charge 5-19, 6-7

primary DLCI 5-11  
Printer Attached 8-11  
Priority 4-5, 4-7, 5-17, 7-14, 7-22, 9-5, 11-5, 11-8  
priority levels 5-11  
Protocol Enabled 5-14  
protocol support 1-2  
protocol, selected for serial port 2-13  
protocols 2-18  
Proxy ARP 9-8  
PU Configuration 7-7  
PU LLC2 Configuration 7-10  
public data network (PDN) 4-3  
PVC Connection 9-7, 10-7

## R

rate parameters 5-7  
rebooting 2-34  
Receive Clock from DTE 5-6, 6-6, 7-6, 8-5  
Receive Not Ready (RNR) 6-10  
Redirect Busy 4-4, 4-7  
redirect options 4-6, 4-8  
Redirect Out-of-Order 4-4, 4-7  
Reject (Rej) 6-11  
reject frames 2-27  
Remote Subscriber ID 7-9, 7-25, 8-8  
Reply Timeout 7-16  
Retransmission Period 8-3  
Retries in Sequence 7-16  
Retry Count 7-9, 8-8  
Retry Sequence Interval 7-16  
Retry Sequence Repeat Count 7-17  
Retry Time 7-9  
Retry Timer 8-8  
RFC 1356 6-1  
RFC 1490 5-1  
RIM Frames 7-17  
Ring Voltage/Frequency 12-4  
RIP 1 Compatible 9-1  
RIP Age Timer 10-8  
RIP Delta Updates 9-5  
RIP Enabled 10-7  
RIP Full Updates 9-5  
RIP Max Size 10-9  
RIP Support 9-7, 9-11  
RIP Version 9-1  
RIP Version 2 9-1  
RIP/SAP Minimum Delay 10-2  
RLP displays 2-2, 2-4  
RLP status 2-17

RLP Thresholds 2-29  
 RNR Limit 7-17  
 Round Robin 4-4  
 Route Metric Hops 9-4, 9-10  
 Router Address 10-13  
 Router Name 10-2  
 routing path 4-5  
 Routing Subscriber ID 7-23  
 Routing Table 4-5, 4-7  
 routing table entry 4-5

## S

SAP Age Timer 10-8  
 SAP Enabled 10-6  
 SDLC Link Station Configuration 7-15  
 SDLC Port Configuration 7-2  
 SDLC Port Statistics 7-26  
 SDLC PU Configuration 7-7  
 SDLC PU LLC2 Configuration 7-10  
 SDLC Status 7-26  
 SDM 12-7  
 Secondary Address 9-9  
 Sequence Number 9-10  
 serial port displays 2-3  
 serial port status information 2-4  
 Serial Port Thesholds 2-30  
 Serialization Enabled 10-6  
 Service Name 10-11  
 Service Type 10-11  
 Session Type 7-20, 11-6  
 Set Asynchronous Balanced Mode (SABM) 6-9  
 Setup Packet Window Size 5-18, 6-4  
 Setup Timer 6-4  
 Severity (traps) 3-2  
 SIM Frames 7-17  
 Single User VC 8-10  
 slow poll list 8-4  
 Slow Poll Retry Count 8-4  
 Slow Poll Retry Frequency 8-4  
 SLT Timeout 12-10  
 SmartSwitch 1800, description 1-1  
 SNA port configuration 7-2  
 SNMP traps 3-1  
 Socket Number 10-11  
 Source Address 9-6, 9-10  
 Source DLCI 9-7, 10-7  
 Source MAC Address Mask 7-23  
 Source Port 9-7, 10-7  
 Source RLP 9-7, 10-7

Source Route Bridge ID 11-2  
 Source Subscriber 9-6, 10-5  
 Speed 2-15, 6-3, 12-12  
 Speed Dial Configuration 12-5  
 Speed Dial Digits 12-6  
 spmarun 2-1  
 Start Synchronization Characters 8-3  
 State 5-11  
 Static Routes 10-10  
 Statistics  
     LAN Card Health 2-27  
     RLP Health 2-24  
     Serial Port Health 2-26  
 Statistics, Voice 12-18  
 Status 2-17  
 Subscriber ID 4-1, 4-3, 4-6, 4-8  
 Subscriber Table 2-9, 4-3  
 Suppression 12-13  
 SVC Idle Timer 9-7, 10-5  
 SVC Retry Timer 9-7, 10-5  
 Switched Virtual Circuits 4-1  
 System Contact 2-16  
 System Description 2-16  
 Systematic Redirect 4-4, 4-7  
 system-level changes 2-34, 5-15, 7-24, 7-26

## T

T1 Link Integrity Timer 5-4, 5-5  
 T1-LLC2 Reply Timer 7-12  
 T1-Reply Timer 7-21  
 T2 Polling Verification Timer 5-5  
 T2-Rcv Ack Timer 7-13  
 T2-Recv Ack Timer 7-21  
 TE Timer 12-9  
 technical support 1-7  
 Telephony Type 12-13  
 Thresholds 2-29  
     Port statistics 2-29  
     RLP statistics 2-29  
 Throughput Class Negotiation 5-19, 6-7  
 Ti-Inactivity Timer 7-12, 7-22  
 Tone Type 12-14  
 TPAD 8-6  
 Traffic Group 7-19  
 traffic priorities 4-5  
 Trailing Pad Characters 8-3  
 Transmit-Receive Capabilities 7-17  
 Transparent Text Support 8-11  
 Transparent Text Supported 8-4

Transport Time 10-7  
trap descriptions 3-4  
traps 3-1  
    and integration 3-1  
    severity levels 3-2  
Tw-LPDUs Outstanding 7-22  
Tw-Max Out LPDUs 7-13

## **U**

Universal LIC 2-18  
Un-numbered Acknowledgment (UA) 6-9  
Unnumbered Interface 9-8  
Use EBCDIC 8-4  
Used Buffers 2-26  
Utilities 1-4

## **V**

Virtual LAN ID 11-2  
Voice Interfaces 12-15  
Voice Node Number 12-2  
Voice Parameters 12-2  
Voice Ports 12-8  
Voice Statistics 12-18

## **W**

Wait Timer 5-14  
WAN Enabled 10-6  
Watchdog Spoofing 10-7  
wildcard characters 4-3